Delphi 7 • Kylix 3 • BugBear • Mac OS X • Telecentros

PC MASTER

Edição 66 • Ano 6 • Brasil R$ 11,90 • Europa 4,50 €

EDITORA 15 EUROPA

www.europanet.com.br

EXCLUSIVO LINUX Mandrake 9

- O Linux mais fácil de instalar
- Traz seis interfaces diferentes
- Configuração rápida e prática
- Todos os pacotes atualizados

2 CDs-ROM Destacando

- Kernel 2.4.19
- KDE 3.03
- Apache 1.3.26
- PHP 4.2.3
- OpenOffice 1.0.1
- Koffice 1.2
- Xfree 4.2.1
- Mozilla 1.1
- GIMP 1.2.3
- MySQL 3.23
- Black Box 0.62
- WindowMaker 0.8

Guia prático do SERVIDOR Windows e Linux

Tudo o que você precisa para rodar as aplicações mais importantes de qualquer servidor com Linux ou Windows

• Servidor Web • Servidor FTP • Servidor de Arquivos
• Acesso Remoto • PPoE Banda Larga • Proxy Server
• Compartilhar Conexão • Servidor de Impressão

Plan9 x Passport

O mundo do software livre desafia mais uma vez a Microsoft. Tudo sobre a nova batalha

VB .NET Fácil

Domine a ferramenta mais utilizada do .NET com o nosso tutorial para iniciantes

Vídeo Digital

O DivX já era. XviD é de graça e tão bom quanto. Conheça melhor esta novidade

NIS passo a passo

Administre sua rede usando apenas um Linux para autenticar usuários de forma rápida e simples

ISSN 16786991

Uma nova geração
de computadores
acaba de nascer.
Computadores
a partir de:
US$ 496,40*
Garantia de 3 anos.
* Dólar comercial, cotação do dia da compra, sob consulta.
Televendas para todo o Brasil 0800 772 72 51
Systemax

DESTAQUES

Servidores
Saiba como montar diversos tipos de servidores de rede. São soluções para servidor Web, FTP, de arquivos, de impressão e muito mais 18

VB .Net
Orientação a objetos e novas tecnologias de acesso a banco de dados são algumas das novidades do VB .NET 38

Mandrake Linux 9.0
Experimente a nova versão da mais popular distribuição Linux, que você recebe nos CDs desta edição ...44

Antes de usar os CDs
Os sistemas Linux e programas distribuídos nos CDs que acompanham a PC Master são indicados para usuários avançados. É altamente recomendável fazer um backup dos dados importantes do seu PC, antes de iniciar a instalação de qualquer Linux ou programa.

Repórter 6
Plan 9 14
XviD 16
Delphi 7 26
Kylix 3 28
Mac OS X 30
Vírus do Mês 32
Rede vulnerável 34
Autenticação NIS 50
O especialista: Alta disponibilidade 56
Falhas de Segurança 58
Família Linux 60
Help Line 62
Crônica: Fazer e Desfazer 66

Se For o Caso, Reclame. Nosso Objetivo é a Excelência!

EDITORA 15 ANOS EUROPA

CORRESPONDÊNCIA
Rua M.M.D.C., 121
CEP 05510-021
São Paulo – SP
Fax: (0xx11) 3819-0538

Atendimento (0xx11) 3038-5050 (São Paulo),
0800-557667 (Outras localidades) – Fax (0xx11) 3097-8583
Das 8h às 20h; sábados das 9h às 15h
e-mail: atendimento@europanet.com.br

Suporte técnico (0xx11) 3038-5070
Horário de atendimento de Segunda à Sexta
das 9h às 12h e das 13h às 17h
e-mail: suporte@europanet.com.br

Redação
Fone (0xx11) 3038-5079
Fax (0xx11) 3819-0538
e-mail: pcmaster@europanet.com.br

Publicidade
Fone (0xx11) 3038-5098
Fax (0xx11) 3819-0538
e-mail: publicidade@europanet.com.br

Para entrar em contato com a Editora Europa
Fones: (11) 3038-5050
São Paulo – SP
ou 0800 557667
Ligação gratuita – Outras localidades
Visite nosso site:
www.europanet.com.br

PC MASTER

Edição Nº 86 – Novembro 2002

Diretores
Aydano Roriz e Abilio P. Cunha

Editor e Diretor Responsável: Aydano Roriz

Redação
Diretor Editorial: Roberto Araújo
Redator-chefe: Luiz Siqueira
Editora-assistente: Angela Nunes
Redator Técnico: Edson Ogihara
Chefe de Arte: Welby Dantas
Assistente de Arte: Rodrigo Mota
Revisão de Texto: Leticia Bueno
Jornalista Responsável: Roberto Araújo MTb.10.766
Colaboraram nesta edição: Ademir Mota, Domingo M. Montanaro, Rodrigo Galan, Fernando Lozano, Sulamita Garcia, Leandro Calçada, Sérgio Vinicius e Toni Cavalheiro

Produção do CD-ROM: Edson Ogihara e Luiz Siqueira
Euroimagem: Valerio Romahn
Internet: Luiz Siqueira (Web Editor) e Cassio Narciso (Web Master)

Diretor Operacional: Abilio P. Cunha

Propaganda: Leticia Nunes

Publicidade São Paulo
Ligue (0xx11) 3038 + ramal desejado
Gerente de produto: Rodrigo Cunha (r 5097)
Executivo de contas: Alessandro Donadio (r 5095) - Flávia Pinheiro (r 5105)

Publicidade Outras Praças
Brasília (0xx61) 242-9590 - New Business
Minas Gerais (0xx31) 291-6751 - Celia de Oliveira
Nordeste (0xx71) 929 - 6624 - Ângela Freitas
Paraná (0xx41) 224-6313 - Helenara Andrade
Rio de Janeiro (0xx21) 507-8541 - Leopoldo Amorim
Rio Grande do Sul (0xx51) 3233-1587 - Rose Isoppo
Santa Catarina (0xx48) 247-7804 - Atanil de Medeiros

Publicidade EUA e Canadá: Global Media
Fone 001 (650) 306-0880; Fax: 001 (650) 306-0890

Circulação e Promoção: João Alexandre, Ézio S. Vicente, Jackeline Monjarás, Joelma Dantas e Marcelo Diniz

Atendimento Pessoa Jurídica: Joelma Dantas (r. 5104) joelma@europanet.com.br

Desenvolvimento de Pessoal: Tânia Marília Ribeiro

Atendimento ao Assinante
Telefone São Paulo: (0xx11) 3038-5050;
Telefone outros estados: 0800-557667
Cecilia Tomazelli (Gerente); Fabiana Lopes (Coordenadora); Carla Dantas; Elisangela Tokashiki; Luiz Eduardo Soares; Paula Hanne; Renata Kurosaki, Erick Melo, Ronie de Souza, Willians Lima da Cruz, Raphael de Oliveira Gherarde e Vinicios Dell'Erba Christe

Suporte Técnico (0xx11) 3038-5070 – E-mail: suporte@europanet.com.br
Marco Clivati (Coordenador); Diogo Cavaletti, Ivan Bastos, Rodolfo Mello, Rodrigo Galan

PC Master (ISSN 1414-3828) é uma publicação mensal da Editora Europa Ltda. O CD-ROM é parte integrante desta edição, não podendo ser vendido separadamente. A Editora Europa não se responsabiliza pelo conteúdo dos anúncios de terceiros.
Números anteriores – No seu jornaleiro ou na Editora Europa
Rua M.M.D.C nº 121 – São Paulo, SP - CEP 05510-021,
Fone 0800 55 7667, Fax (0xx11) 3097-8683
Pela Internet www.europanet.com.br
E-mail atendimento@europanet.com.br

Distribuidor Exclusivo para o Brasil
Fernando Chinaglia Distribuidora S. A. – Rua Teodoro da Silva, 907
CEP 20563-900 Rio de Janeiro - RJ

Distribuição em Portugal:
MIDESA PORTUGAL S.A.
Rua da Republica da Coreia, 34 - Ranholas
2710-460 - Sintra - Lisboa - Portugal
Fone: 21 926 78 00
e-mail: editores@midesa.pt

Impressão: Gráfica Globo Cochrane

ANER – Somos Filiados à ANER –
Associação Nacional dos Editores de Revistas

IVC – Instituto Verificador de Circulação

Ao Leitor

Naquele momento foi uma cartada no escuro. Mas resolvemos correr o risco de colocar nas bancas brasileiras pela primeira vez um CD-ROM com Linux. O imediato sucesso – as vendas da sua PC Master triplicaram em bem pouco tempo – deixava claro o enorme interesse que o sistema despertava. Isso aconteceu em 1999.

Hoje temos o grande prazer de distribuir a versão 9 do Mandrake. Este sistema operacional, junto com o Red Hat (mais usado em servidores) e o Conectiva (que tem boa aceitação tanto em servidores como em PCs domésticos), está rodando hoje num número bem representativo de máquinas por este Brasil afora.

Também neste meio tempo a PC Master se consolidou como a melhor e mais barata forma de qualquer usuário ter acesso a um Linux, tanto em novas versões, como para upgrade. Pode procurar. Você não achará nada mais em conta, mais atual, com instruções em português de instalação e detalhes de uso, do que os sistemas operacionais que distribuímos. Não deixa de ser fabuloso sair de casa com apenas R$ 11,90, ir a qualquer banca e voltar com um Mandrake 9 como você, prezado leitor, acaba de fazer.

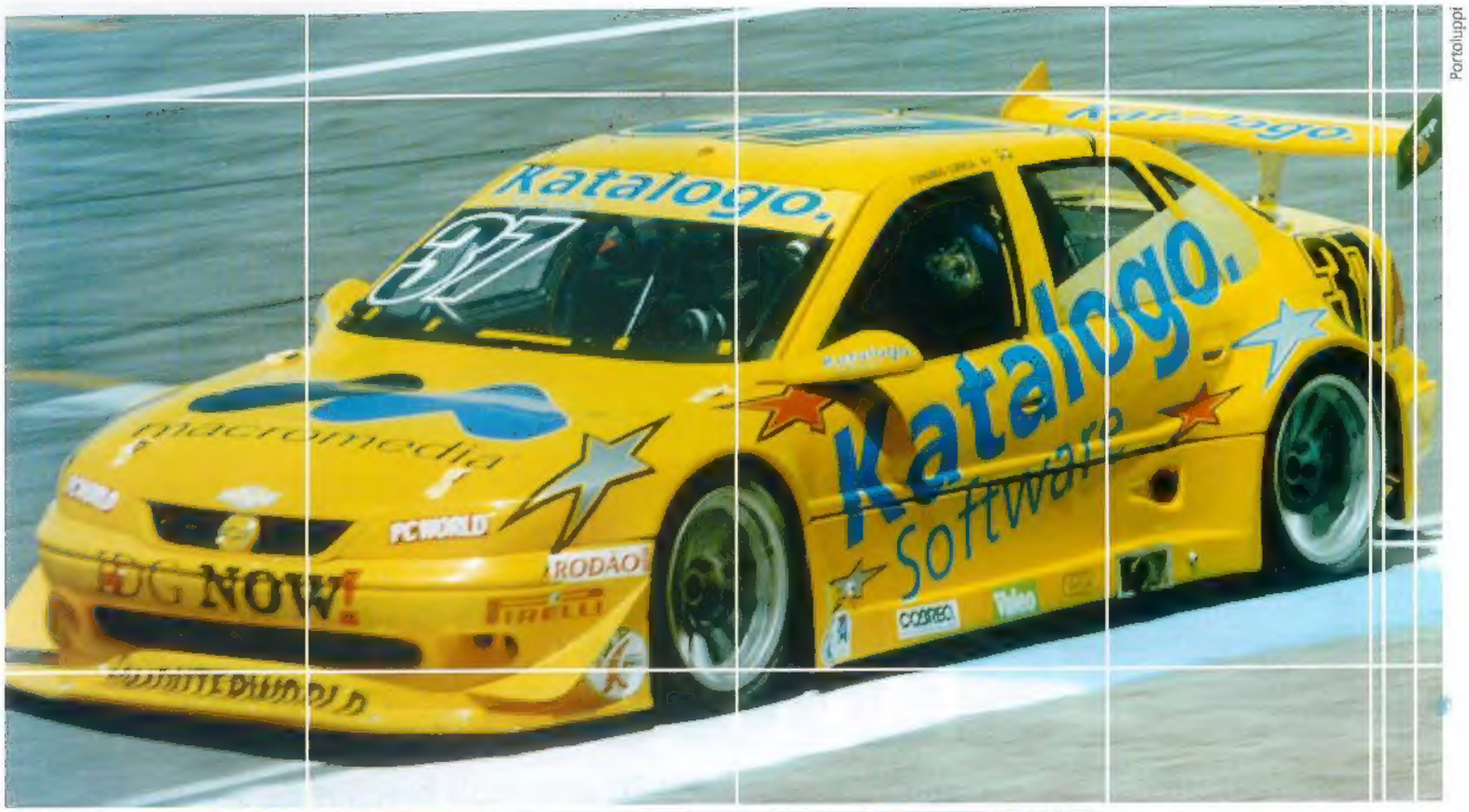
Também, como nos comprometemos lá atrás, o Windows continuou e continuará em nossas páginas. Por mais que você, ou nós, goste de Linux, não é razoável ignorar a importância do Windows. Por exemplo, o Guia Prático do Servidor que fizemos nesta edição contempla todo tipo de usuário, tanto de Linux como de Windows. Cuidamos também para que o nível de conhecimento pressuposto para realizar o trabalho seja bem básico. Agora, se alguém não souber o que é um servidor FTP, decididamente está na revista errada.

Não posso deixar de recomendar também que você experimente o XviD. Se você estiver acostumado com o DivX vai se sentir bem a vontade com seus vídeos digitais usando este novo programa. E com a enorme vantagem que o XviD é de graça.

É por este conjunto de serviços que me sinto totalmente à vontade em afirmar que a PC Master é hoje uma referência entre os usuários avançados. E garanto que você não precisa ficar procurando novidades em outros canais ou revistas. Afinal, você, prezado leitor, nos paga para isso.

Roberto Araújo – Diretor Editorial
araujo@europanet.com.br

Portolupi



Nova Linha Macromedia MX

Com preços imbatíveis!

STUDIO MX
Português

Preço de Mercado:
R$ 2.969,00

Nosso Preço:
R$ 2.519,00

DREAMWEAVER MX
Português

Preço de Mercado:
R$ 2.024,00

Nosso Preço:
R$ 1.258,00

FLASH MX
Português

Preço de Mercado:
R$ 2.503,00

Nosso Preço:
R$ 1.599,00

FIREWORKS MX
Português

Preço de Mercado:
R$ 1.538,00

Nosso Preço:
R$ 943,00

** Os produtos divulgados estarão sujeitos a alteração de preço e a disponibilidade de estoque.*

Katalogo.com.br
Vendas Brasil:
0800-171154
Vendas Rio de Janeiro:
(21) **2264-7117**

Patrocinador Oficial
Katalogo. Software Racing

Seu canal de compra de software!
Mais de 3000 produtos com 150 fabricantes.

Katalogo.®
Professional Software

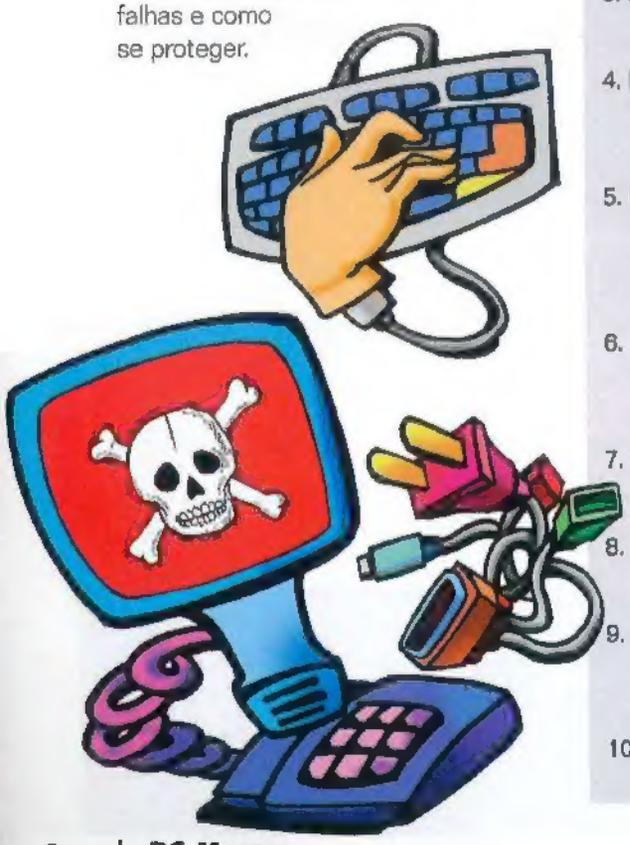
Repórter

Fique por dentro das últimas notícias de informática no Mundo. Entre elas, está a lista divulgada pelo FBI com as principais falhas do Windows e do Linux

As falhas mais graves de 2002

Governo americano divulga sua lista anual das 20 principais brechas de segurança dos sistemas operacionais Unix e Windows. Veja aqui a lista das vulnerabilidades

A agência de segurança americana, FBI, divulgou recentemente as principais falhas de segurança Windows e Unix deste ano. A seguir você confere a lista das vulnerabilidades. No site www.sans.org/top20/ é possível encontrar informações detalhadas sobre as falhas e como se proteger.



Windows

1. **Internet Information Services:** Ao causar buffer overflow, permite rodar comandos remotamente, visualizar arquivos e indisponibilizar serviços.
2. **MS Data Access Components:** Em versões mais antigas, comandos podem ser executados localmente com privilégio de administrador.
3. **Microsoft SQL Server:** Há meios de acessar informações remotamente e de alterar os índices da base de dados.
4. **NETBIOS – Compartilhamento da rede Windows:** Estações remotas podem acessar arquivos e diretórios compartilhados como se fossem locais.
5. **Logon Anônimo - Sessões Nulas:** No Windows NT, 2000 e XP é possível obter acesso aos dados sem login, por sessões nulas destinadas somente à comunicação entre serviços.
6. **Proteção de Senhas Fracas no LAN Manager:** A autenticação do LAN Manager permite que as senhas de rede sejam quebradas por força bruta.
7. **Senhas Fracas ou Inexistentes:** Senhas fracas ou inexistentes, permitem ataques mais facilmente.
8. **Internet Explorer:** É possível esconder exploits em páginas Web que tornem o sistema indisponível.
9. **Acesso Remoto ao Registro:** Configurações impróprias de segurança permitem que o registro seja lido e alterado remotamente sem permissão.
10. **Windows Scripting Host:** Permite a execução de vírus como o *I Love You*.

Unix

1. **Remote Procedure Calls:** Permite que um usuário execute comandos remotos com privilégios de root.
2. **Apache Web Server:** Pode ser atacado com exploits.
3. **Secure Shell:** Algumas versões são vulneráveis a cavalos de tróia.
4. **Simple Network Management Protocol:** Ataques com exploits tornam indisponíveis dispositivos monitorados e configurados através deste protocolo.
5. **File Transfer Protocol:** Falhas permitem acesso remoto como root, e as senhas de login podem ser roubadas pela rede local com um sniffer.
6. **R-Services e Relacionamentos de Confiança:** A falta de criptografia nos "comandos R" permite roubo de senhas.
7. **Line Printer Daemon:** Em algumas versões é possível executar comandos remotos com privilégios de root, através de ataques de buffer overflow.
8. **Sendmail:** Permite acesso ilimitado ao sendmail para o envio de spam com ataques de buffer overflow.
9. **BIND/DNS:** Servidores de nomes podem sofrer ataques como negação de serviço (DoS) e ataques que permitam a execução de comandos sem autorização.
10. **Senhas Fracas ou Inexistentes:** Podem ser descobertas facilmente através de ataques de força bruta.

GNU/Linux

Pingüim para todos

Telecentros de São Paulo implantam sistema Linux e recebem a aprovação de Richard Stallman

Um projeto para inclusão digital em São Paulo está implantando dezenas de centros populares de acesso à Internet na cidade. Nesses telecentros, qualquer pessoa pode, além de navegar de graça na Rede, aprender informática, pois são ministrados diversos cursos para os interessados.

Até agora, já existem 19 centros funcionando e, desde o mês passado, todos eles passaram a operar com o sistema do pingüim. Com a substituição do Windows pelo software livre, estima-se uma economia de R$ 1,5 milhão até o final deste ano e cerca de R$ 2,5 milhões em 2003.

Os telecentros contam com instrutores à disposição dos usuários durante todo o período de funcionamento, além de oferecerem diversos cursos de informática e uma conta de e-mail para os usuários. Tudo gratuito.

Richard Stallman, fundador do projeto GNU/Linux, esteve recentemente em São Paulo para o lançamento do projeto de mudança para software livre nos telecentros. Depois de conhecer o projeto, Stallman ficou tão bem impressionado que passou a indicar a iniciativa paulista como exemplo de migração de sucesso.

Graças a essa indicação, a prefeitura de São Paulo, responsável pelo projeto, foi procurada por técnicos indianos envolvidos num projeto semelhante, os Centros de Informação Comunitária (CICs), na Índia.

Por enquanto, os CICs indianos rodam o sistema operacional Windows e aplicativos proprietários mas, seguindo o exemplo de São Paulo, pretendem substituir os softwares pagos por aplicativos open source.

Nos telecentros paulistas, o objetivo é expandir esses centros e implantar, até 2003, mais 80 unidades, priorizando as periferias da capital. Cada unidade dos telecentros, seguindo o modelo das já em funcionamento, terá 20 computadores, todos com conexão a Internet de alta velocidade, além de todo suporte técnico e pedagógico aos interessados.

Frases

"Unidos podemos enfraquecer o Linux"

Steve Ballmer, CEO da Microsoft, durante conferência Most Valued Professionals evento voltado a desenvolvedores, revendedores e profissionais certificados.

"Há seis ou oito meses, a maior preocupação dos nossos usuários eram os vírus. Agora, o spam é a prioridade"

John Harrington, diretor de marketing da MessageLabs nos EUA. A empresa britânica divulgou estudo afirmando que 17% de todos os e-mails da Rede são spam.

"Paguei minha dívida com a sociedade. Não estou interessado em hackear ou voltar para aquela vida. Aprendi minha lição"

Kevin Mitnick, um dos mais famosos hackers do mundo, que está lançando o livro "A arte do engano", uma ficção com pitadas de autobiografia.

"Eles não estão roubando códigos, mas produtos. Mas os programas ainda estão cheio de bugs e causarão problemas"

Rick Miller, porta-voz da Microsoft, em comunicado oficial da empresa sobre hackers que conseguiram invadir o servidor de beta testes do Windows. Ele afirmou, porém, que os invasores não conseguiram acesso ao código-fonte de seu sistema operacional.

Dos mesmos desenvolvedores do WinRoute.
KerioMailServer5
for secure email communication

A nova geração de servidores de email para redes corporativas.

Gerencie suas contas de email e evite ao mesmo tempo o crescimento das ameaças de segurança em sua rede, através da proteção dos emails de seus usuários.

Outras facilidades

- Web Mail
- Anti-vírus integrado ao servidor
- Filtro de anexos para email
- Anti-Spam
- Back-up
- Pastas públicas
- Suporte multi-domínio

Windows • Linux i386 • Linux PPC • Sun Solaris • MacOS

entre outras...

cadastre sua revenda

www.kerio.com/br

KERIO

vendas@kerio.com.br

Ligue agora 3471-0008

Pirataria

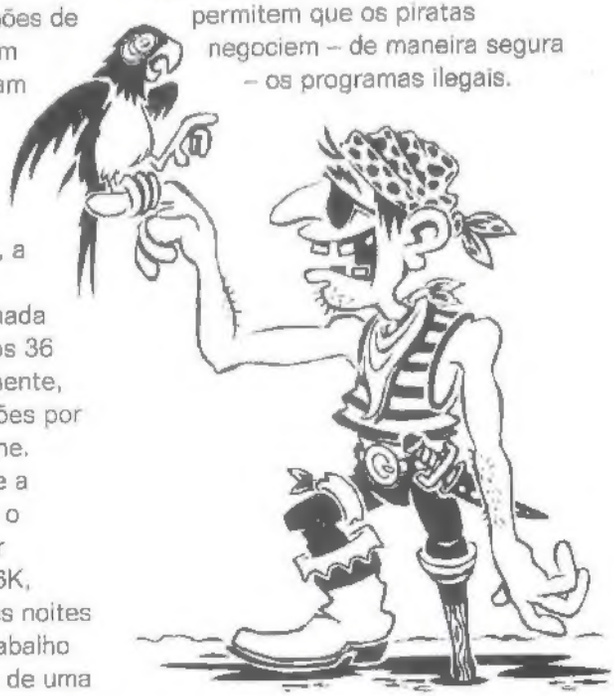
2 bilhões de páginas ilegais

Comércio e distribuição de softwares piratas pela Internet atingiu níveis alarmantes, afirma estudo

De acordo com dados publicados pela Microsoft, existem atualmente mais de 2 bilhões de páginas na Internet que oferecem softwares ilegais ou disponibilizam links para sites com conteúdo pirata. Para a gigante de tecnologia, a pirataria está totalmente fora de controle.

De acordo com a Microsoft, a quantidade de páginas com conteúdo ilegal multiplicou-se nada menos que 20 vezes nos últimos 36 meses – e a culpa é, principalmente, do desenvolvimento das conexões por banda larga e do comércio online.

Isso teria acontecido porque a velocidade de conexão facilitou o trabalho dos piratas. Antes, por exemplo, com um modem de 56K, eram necessárias em média três noites para distribuir um programa, trabalho que consome apenas uma hora de uma conexão rápida. Além disso, os sistemas de comércio eletrônico permitem que os piratas negociem – de maneira segura – os programas ilegais.



CURTAS

Jogo assassino

Um sul-coreano morreu após passar por uma maratona de 86 horas jogando no computador sem parar, sem comer e sem dormir. O homem, que estava desempregado foi encontrado já morto, no banheiro de um Ciber Café, em Kwangiu, na Coréia do Sul.

Wireless

Nos próximos três anos a tecnologia de comunicação sem fio vai crescer em média 27% no mundo todo. É o que aponta um estudo realizado pelo Giga Information Group. De acordo com as estimativas, na América Latina, o uso de wireless vai passar de 21% em 2002 para 31,8% nesse período. Junto com a China e a Índia, será o crescimento mais acentuado.

Bluetooth

Na onda da comunicação wireless, a Microsoft liberou a implementação da tecnologia para redes sem fio de curta distância para seu sistema operacional. Fabricantes de equipamentos agora têm acesso ao software necessário para estabelecer a comunicação com computadores que tenham o WinXP instalado. Sem a liberação desse aplicativo, as empresas de hardware criavam implementações próprias, o que muitas vezes eram incompatíveis.

Para completar a rendição ao Wireless, a MS aproveitou para lançar também – no mercado norte-americano – seu primeiro "pacote" Bluetooth. O kit, composto de teclado e mouse sem fio, além de dispositivo e softwares para comunicação com outros equipamentos, custará cerca de US$ 150.

Crime

Garçom vigarista

Abraham Abdallah admite que roubava dados financeiros e pessoais de personalidades

O que personalidades tão diferentes como Paul Allen, Warren Buffet, Steven Spielberg, Ted Turner, Oprah Winfrey e Michael Bloomberg têm em comum? Aparentemente nada, não fosse o fato de que todos eles tiveram seus dados roubados por um garçom americano.

Abraham Abdallah usou computadores e telefones públicos para invadir contas correntes, criar contas bancárias fraudulentas e conseguir dados pessoais e financeiros de inúmeras personalidades nos Estados Unidos, obtendo históricos de transações, números de cartões de crédito e senhas. A polícia acredita que seja o maior roubo do gênero na história. Para as autoridades, os dados colhidos por Abdallah seriam usados em um esquema para roubar um total de 80 milhões de dólares.

O garçom – preso no início de 2001 com 800 cartões de crédito fraudados e outros 20 mil cartões de crédito em branco – admitiu sua culpa nas 12 acusações que pesavam contra ele, entre elas, roubo de identidade e fraude de cartões de crédito, mas jura que seu propósito não era financeiro.

De acordo com suas declarações, Abraham estaria tomando drogas para distúrbios obsessivo-compulsivos e antidepressivos. Ele só teria cometido o crime não movido pelo dinheiro, mas graças a uma compulsão. Então tá.

Cupido

De acordo com uma pesquisa recente da Ipsos-Reid quase metade dos americanos (44%) acreditam que é mais fácil encontrar um parceiro pela Internet do que em bares e danceterias. Além disso, para mais de 30%, os relacionamentos surgidos através da rede têm mais chances de dar certo do que os iniciados na "balada" e 27% recomendam o uso da Internet para encontrar sua cara metade.

EUA contra censura

Os Estados Unidos levaram ao Congresso um projeto de lei que visa coibir a censura estrangeira a sites da Internet. O projeto propõe a criação de um escritório para a "liberdade mundial na Web" com o objetivo de apoiar e evitar qualquer punição a usuários de países nos quais o governo costuma censurar sites com conteúdo "inapropriado", como acontece freqüentemente na China, por exemplo. O projeto prevê ainda investimentos de US$ 100 milhões, nos próximos dois anos, em tecnologia antibloqueio.

McPornô

Quem costuma fazer uma boquinha no McDonald´s já se acostumou com o acesso gratuito a Internet oferecido por grande parte da rede a seus clientes. Mas é bom tomar cuidado: na Escócia, uma das lojas de fast food suspendeu o serviço. E o motivo foi uma reclamação: os usuários acessavam sites pornográficos – e a loja estava repleta de crianças. Por precaução, mesmo antes do incidente já não era possível entrar em sites pornográficos. Mas para fugir do controle, os usuários abriam anúncios contendo cenas de sexo explícito.

LinuxMall

Sempre conectada com você

Hardware

Roteador Wireless 3x R$ 406,00 ou 1220,00

Gabinete Lavita 3x R$ 92,00 ou 276,00

*Estes preços podem variar devido à oscilação do dólar

5% OFF

COMPRAS POR BOLETO

Acessórios

Camiseta Hackers - Código de barras.

R$ 16,90

Livros

Importados e nacionais!

- Programação (C++, Perl, Ruby, etc.)
- Firewalls em Linux;
- Postfix, sendmail;
- Apache;
- Slackware, Red Hat;
- FreeBSD e outros.

Tel: (11) 5087-9441
Tel/Fax: (11) 5083-8259

www.linuxmall.com.b

SO

Guerra ao Linux

Microsoft admite que sistema operacional do pingüim é uma ameaça para a empresa

"Fomos vencidos pelo Linux em sistemas de alta-capacidade, mas temos uma enorme equipe de desenvolvimento dedicada a contornar isso." Acredite se quiser, essa declaração foi dada por ninguém menos que Steve Ballmer, CEO da Microsoft. Ela aconteceu durante o Microsoft Most Valued Professionals, um evento para desenvolvedores, parceiros e profissionais especialmente certificados, onde a empresa reconheceu o poder da comunidade que desenvolve o sistema Linux, a força da plataforma e a dificuldade de enfrentar sua concorrência.

Ballmer declarou ainda que o sistema do pingüim não vai desaparecer, já que, por não ser uma empresa, e sim uma comunidade, o Linux não depende de dinheiro. "De certa forma, ele já nasceu falido", disse o CEO. Por isso mesmo, a Microsoft quer "criar um senso de comunidade entre desenvolvedores e usuários" para tentar oferecer um sistema adequado para cada mercado e que ofereça vantagens em relação ao software livre.

EM ALTA

SHAWN FANNING

Com apenas 21 anos, o fundador do Napster vai ganhar um filme sobre sua história. A MTV Original Movies decidiu filmar a biografia de Fanning, retratando sua polêmica trajetória, desde a criação do serviço de troca de músicas, até a briga contra a gigante RIAA (associação das grandes gravadoras americanas). Apesar da pouca idade e do curto período de duração de seu site – criado em 1999 –, Fanning revolucionou a indústria fonográfica disponibilizando a troca gratuita de música digital.

EM BAIXA

CDS DA AOL

O provedor de acesso America Online vai receber de volta mais de um milhão de CDs promocionais que distribuiu para clientes e possíveis futuros clientes como amostra de seu serviço. Os responsáveis pelo projeto são dois americanos, John Lieberman e Jim McKenna, indignados com o excesso de CDs enviados pela empresa, que irritam os consumidores e prejudicam o ambiente. Assim que juntarem a "mercadoria", eles enviarão os CDs com a mensagem: "Como você se sentiria se fizessem isso com você?"

4LINUX Men
www.4linux.com.br
Auditoria, Consultoria, Outsourcing e Treinamento.
Fone: +55 11 3889-0108
www.4linux.com.br
contato@4linux.com.br
A empresa de Linux mais Copiada!

Hacker

Dou-lhe uma, dou-lhe duas...

Computadores usados nos anos 90 por um dos maiores hackers da história são leiloados na Internet

Fotos: Divulgação

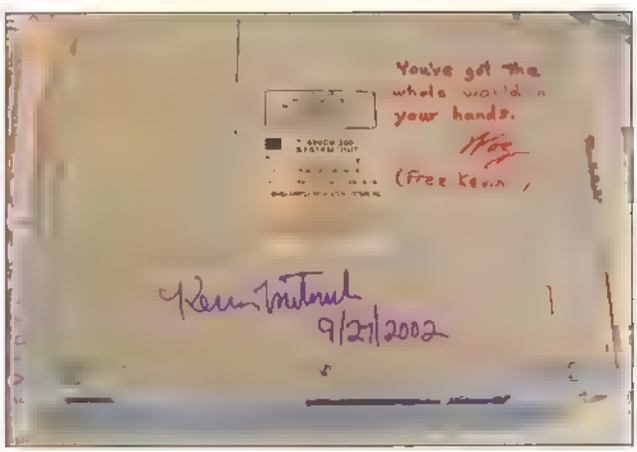
O legendário hacker Kevin Mitnick passou três anos foragido do FBI e outros quatro anos e meio preso, sendo oito meses na solitária. Agora, em liberdade condicional desde 1999, ele está leiloando os laptops que usou para invadir redes de empresas como Novell, Motorola, Sun Microsystems e Nokia.

O Toshiba 1960CS 486, que usava quando foi finalmente capturado, em fevereiro de 1995, foi vendido por US$ 15.200 e o Toshiba Satellite 4400SX, que foi encontrado pelo FBI alguns meses antes – sem seu dono, que escapou por pouco – foi posto à venda com o lance inicial de US$ 6.000. Além de assinados, os computadores ainda possuem a embalagem plástica usada pelo serviço secreto americano para recolher as provas do crime. Mitnick (www.kevinmitnick.com) foi considerado "terrorista da computação" pela justiça americana, que acreditava que ele seria capaz de lançar mísseis nucleares usando um telefone público na prisão.

Hoje, aos 39 anos, dono da consultoria de segurança Defensive Thinking, Mitnick jura que aprendeu a lição, que se regenerou. Mitnick também acaba de lançar o livro "A arte do engano", com histórias fictícias – com uma certa base em dados reais – sobre como manipular e enganar pessoas para descobrir senhas ou mesmo conseguir passar por recepcionistas e guardas.

O dinheiro conseguido com o leilão, de acordo com Mitnick, será usado no pagamento de um advogado para tentar restaurar sua licença de radioamador, que foi revogada enquanto ele ainda estava na prisão. Até 21 de janeiro de 2003, enquanto estiver sob condicional, Mitnick não pode acessar a Internet.

Os dois laptops Toshiba leiloados por Mitnick estão assinados e acompanham embalagem do FBI e um comprovante de autenticidade



RECUPERAÇÃO DE DADOS

HDs, CDs, Disquetes, RAID, ZipDrive ...

Inacessíveis, Defeituosos, Formatados, Bad Block,
Ataque de Vírus, Hackers, Arquivos Corrompidos,
Apagados, Senhas Esquecidas, Clones Físicos ...

Laboratório nos EUA (opcional)

www.doctorbyte.com.br

Av. Iraí 79 cj 125 B - Moema
cep: 04082-000 - São Paulo - SP
Tel 0xx11 5093 7397 / 5531 2370

Cursos e eventos

Network Security
09/11 e 07/12 - R$ 295,00
40h – Universidade Estácio de Sá
O curso apresenta conceitos de redes de computadores, os principais tipos de ataques, política de segurança, firewalls, serviços de segurança, OSI, integridade e confidencialidade dos dados, VPN e Proxies.
Av. Pres. Vargas, 642 - 2º andar - Rio
Tel. (21) 2563-0000
www.ricardoporteiro.com.br/calendario.htm

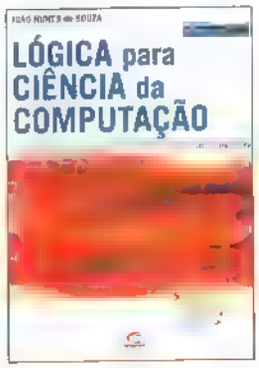
Fenasoft Discount Week
5/11 a 9/11
Expo Center Norte
Feira de tecnologia, produtos e serviços de software e hardware. São grandes marcas, empresas revendedores e varejistas em um evento de vendas no varejo.
Pavilhão Azul, Vermelho e Branco
Rua José Bernardo Pinto 333 - SP
www.fenasoft.com.br

Linux Professional
18/11 a 29/11 – R$ 880,00
40h – Worldtraining
Destinado a quem já possui conhecimentos básicos de sistemas operacionais e uso de computadores pessoais, esse curso ensina como trabalhar com distribuições Linux e configurar serviços existentes, oferecendo o conhecimento necessário para administrar qualquer plataforma Linux do mercado.
Al. Santos, 1893 - 9º andar - SP
Tel. (11) 3285-2224
www.worldtraining.com.br

Eletrônica Analógica
10/11 a 15/12 – R$ 435,00
40h – Impacta
O objetivo desse curso é ensinar os participantes a compreender, consertar e desenvolver circuitos eletrônicos básicos
Av. Paulista, 1009 - 9º andar – SP
Tel. (11) 3285-5566
www.impacta.com.br

Livros

Segurança no Desenvolvimento de Software
Ricardo Albuquerque e Bruno Ribeiro - 320 páginas
Editora Campus - R$ 49,00
Voltado para desenvolvedores, este livro apresenta os principais conceitos e ferramentas para o planejamento correto da segurança de aplicações. Além disso, explica como implementar, melhorar e avaliar os sistemas, garantir que sejam seguros e atendam às necessidades do cliente. É baseado na norma internacional ISSO/IEC 15.408 – Common Criteria for Information Technology Security Evaluation



Lógica para Ciência da Computação
João Nunes de Souza - 328 páginas
Editora Campus - R$ 49,00
Apresenta fundamentos da lógica para estudantes das diversas áreas ligadas à computação. O livro é voltado para quem está cursando o ensino superior, mas não exige nenhum conhecimento específico em matemática. Explica as lógicas Proposicional e de Predicados e traz demonstrações e mais de 700 itens de exercício.

VB .NET - Introdução à programação
Craig Utley - 392 páginas
Editora Berkeley - R$ 52,00
O livro apresenta uma comparação entre VB6 e VB .NET, mostrando as propriedades padrão em uso. Explica também, entre outras coisas, como construir classes e seções com o VB .NET, como iniciar o ADO .NET, migrar de projetos do VB6 para o VB .NET, construir aplicações Web com o VB .NET e com ASP .NET, construir um serviço Web, criar aplicações multithreading e monitorar o desempenho.

Tudo que você queria saber sobre o TCP/IP
Anderson Santos e Fábio Câmara - 112 páginas
Editora Makron Books - R$ 25,00
Os autores demonstram o funcionamento de arquitetura TCP/IP. O livro explica o planejamento de redes de computadores, como fazer configurações dos protocolos e controlar como a informação é passada de uma rede à outra. Também ensina como manipular o endereçamento dos pacotes, a fragmentação dos dados e a checagem de erros.

Hospedagem

Registro de Domínio

E-mail

E-commerce

Soluções...

Sua empresa não existe na Internet?

Venha para a Digiweb Brasil!

Planos de hospedagem a partir de R$ 29,90

Nesses dias de globalização, quem não tem um web site na Internet não existe.

Abra as portas de sua empresa para o mundo, tenha um web site na Internet.

Não fique para trás, na **Digiweb Brasil** você encontra toda a eficiência, rapidez e segurança que você precisa para fazer seu projeto de Internet virar um sucesso. Tudo que você imaginar, web site, portal, megaportal, comercio eletrônico, não importa o que você quer fazer, nós temos a solução do tamanho de sua necessidade.

Na hora de decidir, escolha quem faz mais por você.

Rápido

Fácil

Econômico

Seguro

www.digiweb.com.br

Ninguém está mais preparado para cuidar de seu web site.

Digiweb BRASIL

(11) 5084-2575

Plan 9
das telas para o PC

Microsoft pode ter os planos para seu Passport frustrados pelo Plan 9, o passaporte do pessoal Linux

Por Sérgio Vinícius

A MS lançou o sistema de autenticação Passport há algum tempo. E, com ele, pretende abocanhar cada vez mais internautas e usuários para seus serviços online. Entretanto, a turma do Linux avisa que a empresa de Bill Gates deveria maneirar na empáfia. Isso porque, se a MS tem uma plataforma, afirmam os entusiastas do open source, eles têm um projeto de outro mundo, o Plan 9. O nome, que foi pego emprestado do pior filme de todos os tempos (*veja quadro na página ao lado*), não inspira confiança, mas sua plataforma sim: é uma versão remodelada do Unix combinado com o servidor Apache.

A idéia dos desenvolvedores do Plan 9, assim como o Passport, é criar um serviço no qual os usuários preencham um formulário online com suas informações pessoais uma única vez e depois possam acessar uma série de sites e serviços na internet sem a necessidade de se cadastrar novamente em cada um deles.

Entre os sites parceiros do Passport estão, por exemplo, o Starbucks.com (www.starbucks.com) e as páginas da MSN, que também pertence ao grupo Microsoft. Para o Plan 9, por sua vez, estuda-se sua utilização no Projeto Liberty (www.liberty.org), capitaneado pela Sun Microsystems.

Passport

Para garantir que o Passport funcione em conjunto com serviços de competidores e sistemas proprietários usados por corporações, a Microsoft incluiu suporte a uma tecnologia chamada Kerberos no Passport. O Kerberos é um padrão aberto para transações digitais seguras desenvolvido por pesquisadores do Massachusetts Institute of Technology (MIT). Ao suportar o Kerberos, o Passport interage com todos os outros serviços de autenticação que também utilizam a tecnologia.

Mas ainda na época em que era desenvolvido, já havia muitas dúvidas sobre a viabilidade da idéia da empresa de Bill Gates, já que os grandes rivais da companhia eventualmente se recusariam a participar da iniciativa. "Realmente acho difícil que a AOL participe disso", disse, na época, Chris Le Tocq, analista da Guernsey Research, que acompanhava o desenvolvimento do Passport.

E não era só a AOL que recusaria o sistema. Afinal, a turma do software livre também tem fortes razões (ideológicas, em sua maioria) para ficar com os dois pés atrás com relação a quase tudo que a empresa de Bill Gates coloca no mercado. Então, mesmo antes de saberem do Passport começavam a desenvolver seu próprio passaporte, versão open source.

Plan 9

O Plan 9 foi lançado no final dos anos 80, desenvolvido originalmente pela AT&T Bell Labs, e é fruto do mesmo centro de pesquisas que criou o sistema operacional Unix e as linguagens C e C++.

Passport pode ser aberto

Enfrentando problemas legais e fortes críticas da indústria, a Microsoft anunciou que vai alterar o seu sistema de autenticação Passport, garantindo interoperabilidade com serviços similares oferecidos por empresas rivais.

A desenvolvedora também anunciou planos de entregar o gerenciamento do sistema para um grupo que seria formado tanto por parceiros corporativos como por competidores, além da própria Microsoft.

"Permitir que múltiplos provedores de serviços sejam capazes de atuar em conjunto é uma tremenda oportunidade para a indústria", afirmou Brian Arbogast, vice-presidente de serviços da plataforma .Net da Microsoft. Segundo o executivo, a adição de interoperabilidade no Passport deve acontecer em 2003.

Surgido inic almente como uma forma de autenticação do Unix, o Plan 9 ganhou corpo graças à indústria de software e ao público em geral que responderam bem às iniciativas de d stribu ção de produtos como o navegador Netscape (versão 6), o Darwin (núcleo do Mac OS X) da Apple e o Linux.

Quando foi criado o Unix, as formas de acesso e autenticação do sistema não eram problema: uma senha reso via facilmente isso. Mas o contratempo surgiu quando necess tou-se interligar dois ou mais servidores, e as pessoas precisavam de, no mínimo, duas senhas para entrar nos s stemas. Com o tempo, resolveu-se este problema, mas não de forma completamente segura. Então, o Plan 9 surgiu para solucionar a questão

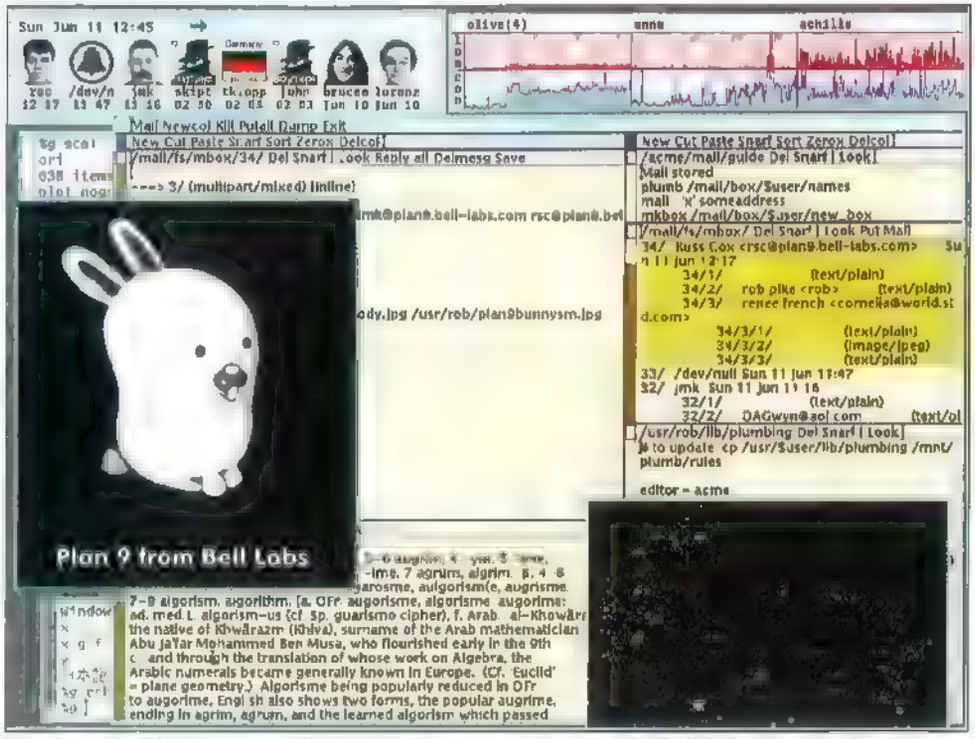
Em operaçao, o Plan 9 parece com um sistema Unix, mas com diferenças nternas em seu desenho – e é justamente essa a característica que o torna a chave que interliga as diferentes máquinas rodando em diferentes s stemas.

Em Unix, a autorização do usuário é definida de acordo com uma máqu na específ ca. O Plan 9, d ferentemente, define a autorização a partir de uma máquina virtual formada por d versas máquinas fis cas, distribuindo e permitindo os acessos.

Além disso, o Plan 9 faz com que o sistema de arquivos seja d sposto ao usuário de forma hierárquica e os acessos às máqu nas sejam trocados ind vidualmente, de acordo com a função. Desta forma, um usuário pode acessar um programa sendo executado ou um CPU servidor sem precisar saber, necessariamente, a go sobre a máquina – como onde ela está, quem é seu proprietário ou qual o tipo de máquina

Liberty, o projeto

Enxergando robustez no Plan 9, o pessoal da Sun tenta incorporar o sitema ao seu projeto Liberty Alliance (www.projectliberty org). A iniciativa tem como objetivo desenvolver um padrão de ident dade digital aberto e interoperável.



Interface do Plan 9 : ponto forte do sistema open source da Bell Labs é sua robustez

A Identidade Digital Federada, ponto principal do Liberty, perm te uma senha de autorizaçao única e descentralizada e permissao aberta para qualquer aparelho conectado à Internet. Entretanto, a segurança para isso é sua pr nc pal preocupação. Coisa que o Plan 9 promete resolver **PCM**

Plan 9, o filme

O nome Plan 9 foi dev damente t rado do filme P an 9 From Other Space, do diretor Ed Wood. A pe cula é considerada o p'or f lme do mundo Na época de desenvolv mento do software os envolvidos no pro eto chegaram à conclusão que tinham idéias bastante esquis tas para desenvolvê- o, e associaram uma co sa a outra.

No filme, extraterrestres tentam o nono plano para domín o da terra, depo s do fracasso dos anteriores. Por razões que o fi.me não esc arece, decidem ressuscitar os recém-mortos

Dal para a frente é uma sucessão de absurdos. Para se ter uma idéia, a verba para rodar o filme foi conseguida de uma greja (aparentemente com o objet vo de gerar recursos para futuros filmes sobre a vida dos apóstolos).

Além disso, o único astro do f lme (Bela Lugosi) morreu logo no início da produção, deixando apenas algumas poucas cenas soltas filmadas. Para subst tu -lo, Wood escalou seu man curo para o papel. Este, por não ter a menor semelhança com o falec do ator, passa o f lme inteiro cobrindo o rosto com uma capa.

Há ainda d scos voadores feitos de calotas de carros penduradas por f os na frente de cenários de papelão d álogos incompreensíve s e uma montagem tosca que não se importa em alternar cont nuamente dia e noite na mesma cena. Por fim, os momentos em que o exército combate os invasores são trechos de documentários enxertados aleatoriamente. Rea mente, um prato che o.

Em tempo: o coelho mascote do projeto se chama Glenda, também em homenagem a outro fi me de Wood, Glenn or Glenda

XviD

O codec realmente free

Conheça tudo sobre o codec de compressão de vídeo verdadeiramente grátis e open source que foi criado para ser uma alternativa ao DivX

O XviD, formato de compressão de vídeo que está conquistando cada vez mais usuários, provavelmente ainda vai conquistar você. Isso porque esse codec, além de totalmente open source, é gratuito de verdade.

Até não muito tempo atrás, o formato preferido dos usuários era ninguém menos que o "arqui-inimigo" do XviD: o DivX. O antigo líder perdeu espaço quando fechou seu código e, mais ainda, passou a cobrar por suas melhores e mais completas versões.

A disputa entre esses dois padrões explica-se não só pela simples concorrência mas também por suas origens. O Projeto XviD foi fundado em agosto de 2001, pelo então estudante alemão Michael Militzer alguns meses depois de encerrado o Projeto Mayo, que desenvolvia o OpenDivX, versão open source do DivX. O Projeto Mayo era realizado pela própria DivXNetwork, a "proprietária" do DivX.

Michael Militzer, que era um dos responsáveis pelo desenvolvimento do OpenDivX, não concordou com a nova política proprietária e decidiu fundar seu próprio projeto e criar um novo codec que fosse realmente aberto e gratuito. "Eu acreditava (e ainda acredito) que existe uma carência pela implementação gratuita, open source e competitiva de padrões tão

importantes e amplamente usados como o MPEG-4", just f ca Mil tzer, que, junto com ele, levou diversos programadores talentosos do Projeto Mayo e assim criou o XviD. Hoje o projeto conta com desenvolvedores no mundo todo.

"Os motivos para o fim do OpenDivX não ficaram explícitos, mas suponho que tenham s do razões econômicas. A DivXNetworks hoje ganha d nheiro vendendo seu codec para o consum dor final ("professional version") e licenciando seus codec (e seu conhecimento) para outras companh as. Essas duas mane ras de ganhar dinneiro são impossíveis, ou no mínimo comp icadas de realizar com o DivX open-source", explica M litzer.

Ainda de acordo com o fundador do XviD, um outro grande problema enfrentado por esse tipo de codec open source é que, por seu alto valor comercial, é mu to d.fícil proteger seu código aberto, que pode ser faci mente roubado por competidores (o caso da XviD contra a Sigma, no quadro ao ado, prova isso).

XviD x Sigma

Durante se s semanas, entre os meses agosto e outubro, o s te do XviD (www.xvid.org) ficou "fora do ar". No ugar de sua página n cial, apresentava um comunicado informando que o desenvo vimento do codec estava parado. O motivo de o projeto ter sido temporariamente interrompido fo uma disputa com a S gma, que util zou indev damente os códigos do XviD. O REALMag c MPEG-4 Video, o codec da S gma, possui diversos trechos do código-fonte original do XviD, mas os termos da licença GPL (GNU Public Licence) e os avisos de copyrigth or g nais foram remov dos. Com isso a empresa v olou não só os direitos autorais, mas um dos mais importantes princípios da GPL, que determina que qua quer programa criado a partir de um software GPL tem de seguir também os termos da licença.

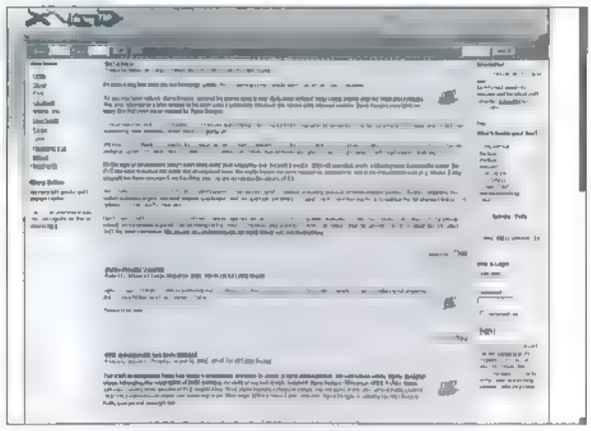
Enquanto tentava resolver esse prob ema – e até que a Sigma parasse de infringir os dire tos autora s do codec – a equipe do XviD dec diu parar seu desenvo vimento Passadas seis semanas, porém como não houve entend mento, o XviD voltou a ativa, mas garante cont nuar brigando, nclusive na just ça, para garantir que a icença seja respeitada

Concorrência

Um dos principais diferencia s do Xv D é a compat b lidade. Existem versões ot mizadas disponíve s para todas as plataformas x86, incluindo W ndows, Linux e BeOS, por exemplo. Alem disso, XviD pode também ser usado em mu tas outras plataformas além das x86, como rix, Sparc, PowerPC e .tanium.

Contudo, bas camente, não há diferenças de formato entre o XviD e o DivX. Ambos são codecs baseados no padrão MPEG-4, portanto, vídeos XviD podem ser rodados com DivX e vice-versa (ao menos em teoria, mas algumas versões antigas do DivX possuem bugs e por isso não reproduzem conteúdos codificados pelo XviD corretamente).

O padrão MPEG 4, assim como outros padrões MPEG, apenas descreve como o processo de decodificação deve ser. Isso significa que o padrão não especifica o encoder (o processo de codificação), que pode ser desenvolvido livremente. Apenas o formato de compressao resultante desse processo deve ser suportado pelo padrão do decodificador. Isso também quer dizer que as soluções de vídeo codec referentes ao MPEG 4 podem diferir .mensamente em termos de qualidade e rapidez.



O XviD é mais rápido e tem maior qualidade visual que o DivX gratuito, mas perde para a versão Pro

Como exemplo, apesar das semelhanças dos dois principais codecs, o XviD é basicamente mais rápido e alcança qua dade visual cerca de 20% ma or que a versao gratu ta do DivX 5

Já a versão profiss onal do DviX 5, que é paga, possui a guns atributos adicionais (principalmente *quarter pixel motion estimation* e frames bidirectionais) que o Xv D ainda não suporta oficialmente. De acordo com Mi .tzer, os desenvolvedores do XviD estão trabalhando na implementação desses diferenciais, mas ainda é preciso a guns outros testes e por sso a nova versão ainda não fo ofic almente liberada

Assim, o DviX 5 profissional e o XviD são frequentemente considerados complementares em termos de qualidade visual. O XviD, entretanto, possui a imensa vantagem de ser cód go livre e por isso, além de possu r um enorme time de desenvo vedores, pode ser adaptado ao gosto do usuário.

"Nós esperamos superar o DivX e apresentar novamente uma melhor performance com o próximo lançamento do XviD", promete Militzer. Entretanto, o pessoal da DivX, certamente, tentará fazer o mesmo. E o vencedor dessa disputa, só o tempo dirá quem será. Por enquanto, quem ganha é o usuário. **PCM**

Guia prático do Servidor

Aprenda como tirar melhor proveito de sua rede adicionando diversos tipos de servidores para rodar as mais importantes aplicações em Windows ou Linux

Utilizando servidores em sua rede você pode melhorar a organização das informações que circulam pela rede, aproveitar os recursos disponíveis e compartilhar sua conexão de banda larga, entre outras coisas, obtendo assim uma redução de custo. Nessa reportagem você verá como tirar um melhor proveito de sua rede adicionando diversos tipos de servidores. Entre os recursos disponíveis você saberá como montar e aproveitar servidores Web, FTP, Proxy, de arquivos e outros mais. Confira.

Conexão PPPoE

O protocolo PPPoE é o sistema de autenticação de usuários para o serviço de banda larga. Sem essa autenticação, o computador não se conecta a Internet para navegar

Windows

No Windows XP não é necessária a instalação de nenhum programa para utilizar o PPPoE, pois ele já vem no sistema operacional. Já nas versões anteriores, é necessário utilizar o aplicativo que está no site http://user.cs.tu-berlin.de/~normanb/. Para configurar a conexão, clique em: *Iniciar*, *Todos os programas*, *Acessórios*, *Comunicações* e *Assistente para novas conexões*.

Na tela que aparecer, serão solicitadas informações sobre a localidade onde você mora. Os demais campos podem ser preenchidos com um "0", já que não será utilizada uma conexão discada para acessar a Internet e sim uma rede. Siga as instruções que forem surgindo e marque a opção *Configurar minha conexão* manualmente.

Marque a opção que indica a conexão com um servidor de banda larga, com o protocolo PPPoE, e em seguida clique em *Avançar*. Preencha a janela com o nome da conexão. Logo em seguida serão perguntados os dados sobre a sua conexão. Preencha os campos e marque as opções necessárias.

Agora a conexão foi criada. Abra o navegador e teste a sua conexao.

Linux

Para a configuração do PPPoE no Linux é necessário que a sua placa de rede esteja instalada e configurada. Use a opção de obter o endereço diretamente do servidor DHCP. Esta configuração faz com que endereco IP, servidor de nomes e gateway sejam obtidos automaticamente do servidor – que nesse caso é o seu provedor Internet.

Também é necessário ter o pacote RP-PPPoE, que você encontra nos CDs da distribuição Mandrake, e recebe nesta edição da PCMaster. Verifique se existem os arquivos */etc/ppp/firewall-standalone* e */etc/ppp/firewall-masq*. Algumas distribuições não trazem esses arquivos por padrão. Caso não os possua, você pode pegá-los no endereço www.europanet.com.br/pcmaster/edicao60.

Depois de instalado o pacote, execute o software de configuração usando o comando: *adsl-setup*. Em seguida, será solicitado que você informe os dados de sua conexão, tais como usuário, senha e servidor de DNS.

Ao terminar a configuração, teste a conexao digitando o comando: *adsl-start*. Se nenhum erro apareceu, sua conexão está pronta para ser usada. Abra o navegador e teste se está funcionando.

Web Server

Você pode instalar em seu computador com banda larga um servidor Web para apresentar seus trabalhos, compartilhar seus documentos e muito mais

Windows

O arquivo de instalação do Apache está disponível para diversos sistemas, como Linux, Windows e Mac. Faça o download do arquivo de instalação do Apache no endereço www.apache.org/dist/httpd/binaries/win32.

Atualmente, a última versão do servidor Apache disponível é a 1.3.27. Para instalá-la, execute o arquivo e siga as instruções que são apresentadas durante o procedimento. Para iniciar o servidor Web Apache nas versões do Windows 9x, Me e XP, vá no botão *Iniciar*, *Programas*, *Apache HTTP Server*. Clique em *Start Apache in Console*. Uma janela deverá aparecer, indicando que o Apache está em execução. Para os usuários do Windows NT e 2000, o servidor Web será apresentado como serviço do sistema. Configure a sua inicialização no Painel de Controle.

Não é aconselhável parar o Apache fechando esta janela diretamente, pois isso pode comprometer o servidor. Vá em *Iniciar*, *Programas*, *Apache HTTP Server* e clique em *Stop Apache*. Este procedimento dará início ao processo de shutdown do servidor Web, o que fará com que a janela se feche.

Para testar a instalação, primeiramente, certifique-se de que o Apache esteja em execução. Abra o seu navegador favorito e digite o seguinte endereço: http://localhost. Uma página de teste deverá aparecer, indicando que você instalou e configurou corretamente o servidor Web Apache em seu sistema.

As páginas que serão apresentadas por seu servidor Web devem ser colocadas no diretório *C:\Arquivos de programas\ApacheGroup\Apache\htdocs*.

Juntamente com o seu servidor Web, você também pode adicionar outros recursos, como ASP e PHP, basta que sejam instalados juntamente com o servidor.

Linux

Faça o download do arquivo no endereço www.apache.org/dist/httpd/binaries e faça a instalação em sua distribuição Linux. É possível encontrar o arquivo binário para a grande maioria dos equipamentos e distribuições de sistema operacional Linux. Normalmente, o software encontra-se disponível no CD da distribuição que você está utilizando. No caso do código-fonte, faça o download do arquivo e siga o seguinte procedimento para compilar o sistema:

```
# tar -xzvf apache-1.X.XX.tar.gz
# cd apache 1.3.12
# ./configure --enable-module=so
# make
# make install
```

Após instalar o sistema, confira os diretórios: */usr/local/etc/apache*, diretório onde se encontram os arquivos de configuração do Apache, e */usr/local/www*, onde seus arquivos *.html* serão armazenados. Para inicializar, digite:

```
# /usr/local/apache/bin/apachectl start
```

É possível startar o httpd automaticamente junto à inicialização do Linux, e este procedimento varia de uma distribuição para outra. Normalmente, deve-se criar um arquivo dentro do diretório responsável pela inicialização (por exemplo, */etc/init.d/*) que contenha a linha de comando anterior e torná-lo executável através do comando:

```
# chmod +x
```

Para realizar a configuração no servidor apache veja o arquivo */usr/local/etc/apache/conf/httpd.conf*. Se desejar, por exemplo, alterar a porta do servidor Web, basta localizar no arquivo a linha correspondente por padrão *port80*.

Dica

Para a versão Windows foi utilizado o servidor Web Apache, mas caso a versão utilizada seja Windows NT ou 2000, pode-se utilizar também o IIS (Internet Information Server), que encontra nativo nestas duas versões de sistema operacional.

Muitas operadoras de banda larga não permitem que se utilize servidor Web e bloqueiam a porta 80. Uma forma de contornar este recurso, é alterar a porta no arquivo de configuração do servidor. Como sugestão, altere a porta do servidor para a porta 81.

Servidor de FTP

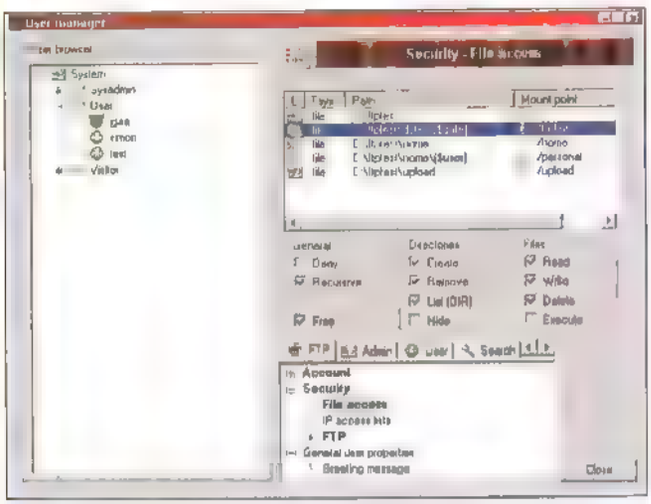
Uma forma simples e segura de compartilhar seus arquivos com outros usuários através da Internet é usando um servidor FTP. Aprenda como fazer isso

Windows

Para montar um servidor de FTP para compartilhar arquivos, será necessário baixar um programa adequado a tal função. Existem diversos softwares que realizam esta tarefa. Duas boas opções são o Serv-U (www.serv-u.com), um shareware que funciona por 45 dias, e o War FTP (www.warftp.org), que se trata de um freeware.

O Serv-U é bem mais simples de se configurar porém o War FTP tem a excelente vantagem de ser gratuito. Faça o download do software escolhido e realize a instalação do aplicativo em seu sistema. Ao final da instalação exeute o software para que o serviço se torne disponível.

Configure o programa cadastrando os usuários que terão acesso. Para isso, forneça os *usernames* e as senhas de quem vai poder acessar o FTP e configure as pastas que cada um vai poder acessar.



O War FTP é uma ótima solução para se montar um servidor FTP e ainda tem a vantagem de ser gratuita

Linux

Um dos servidores de FTP mais comuns para Linux é o servidor WU-FTP (www.wu-ftpd.org). Ele é fácil de gerenciar, basta seguir o passos descritos no arquivo *INSTALL*, contido no pacote da sua distribuição. Independente do servidor FTP instalado, é preciso que o daemon ftpd seja inicializado pelo deamon */etc/inetd.conf*. Adicione a linha abaixo neste arquivo de configuração:

```
ftp stream tcp nowait root/usr/sbin/ftpd  ftpd  lalo
```

No exemplo dado, as opções *-l*, *-a*, *-i* e *-o* fazem com que as sessões sejam registradas ("logadas"), o uso do arquivo *ftpaccess* seja habilitado e as transferências para o servidor também sejam registradas, bem como aquelas feitas a partir do servidor. Estas opções foram consideradas sob a perspectiva de executar o servidor de uma maneira mais segura.

Grande parte da configuraçao do servidor WU-FTP é feita através do arquivo *ftpaccess*. Dentre outras coisas, ele define os usuários e a forma de acesso ao servidor que eles terão, controla as mensagens que serão mostradas aos usuários e define um sistema de logs bastante completo.

O arquivo *ftpusers* contém uma lista de usuários que não podem acessar o servidor via FTP. Este arquivo deverá conter nomes de usuários relacionados ao sistema e não nomes de usuários comuns. O formato do arquivo é um nome de usuário por linha. Desta forma, usuários mal-intencionados não poderão, pelas vias normais, entrar nestas contas via FTP.

O arquivo *ftphosts* trabalha de maneira similar ao arquivo *ftpusers*. A diferença reside no fato de que com ele pode-se especificar quais usuários, de quais máquinas, têm a permissão de acesso bloqueada ou permitida.

É possível também usar wildcards e endereços IP de forma a permitir ou bloquear o acesso a domínios inteiros

Dicas

Caso você esteja usando o provedor de acesso rápido Speedy, não se esqueça de alterar a porta do FTP de 21, que é o padrão, para uma outra, como por exemplo a 1521 ou qualquer porta livre.

Ao se criar um servidor FTP, evite manter os usuários padrões como *anonimous*. Isso permite que qualquer usuário tenha acesso ao sistema.

Sempre monitore o trabalho que vem sendo feito pelo servidor FTP, já que todos os softwares gravam log ou permitem monitoramento.

Central de arquivos

Uma solução para os usuários que trabalham em rede é centralizar todos os arquivos em servidores, evitando problemas como a desatualização de trabalhos

Windows

Para compartilhar arquivos em estações de trabalho Windows XP, basta abrir a pasta *Meus documentos*. Clique no arquivo ou pasta que você deseja compartilhar, arraste o arquivo ou pasta para *Documentos compartilhados*. O Windows XP já compartilha esta pasta por padrão.

Já em estações Windows 9x, e Me, para compartilhar arquivos e diretórios clique com o botão direito do mouse e selecione no menu a opção *Compartilhamento*.

Marque o item *Compartilhamento*, selecione as opções relacionadas, como se será permitida apenas a leitura ou terá compartilhamento completo.

Servidor de dados seguro

Para montar um servidor de arquivos em uma rede Windows, a melhor solução é criar um servidor de domínio utilizando um dos servidores de rede, como o Windows NT ou 2000.

Você deve cadastrar no servidor todos os usuários que utilizam os recursos de rede, criando grupos de trabalho separados por departamentos. Com isso, as estações são obrigadas a validar as senhas dos clientes no servidor, aumentando a segurança das informações.

Ao se compartilhar arquivos e diretórios, verifique na opção *Segurança* as permissões dos grupos e usuários que utilizarão os recursos compartilhados. Para as estações de trabalho que pertencem ao domínio, mesmo o Windows 9x e Me, será carregada a lista de usuários cadastrados no servidor. Assim poderá ser atribuída aos compartilhamentos das estações as mesmas seguranças do servidor.

Este recurso permite que se gerencie todos os usuários que estão conectados em seu servidor, saber quais os arquivos se encontram em uso e também desconectar quando necessário cada um deles.

Linux

Aqui você verá a forma mais comum que permite compartilhar arquivos do Linux para uma rede Windows. Para compartilhar dois diretórios sem restrições de acesso, como por exemplo */home/samba* e */home/comum*, crie os dois diretórios na pasta *home* usando o comando:

```
mkdir <nome do diretório>.
```

É ideal que se guarde uma cópia do arquivo *smb.conf*. Para isso, use o comando:

```
cp smb.conf smb.conf.copia
```

Com um editor de textos, ajuste o arquivo *smb.conf*:

```
[global]
workgroup = seu grupo de trabalho do windows
server string = Servidor Samba
security = SHARE
log file = /var/log/samba/log.%m
max log size = 50
printcap name = /etc/printcap
dns proxy = No
guest account = guest
hosts allow = 192.168.200. 192.168.254. 127.
printing = bsd
[comum]
comment = Pasta comum
path = /home/comum
read only = No
guest ok = Yes
write list = @staff
```

Para se criar um novo compartilhamento, basta adicionar uma nova entrada como a *[comum]*.

Dica!

Se a pasta ou o arquivo que você [illegible] encontrado na pasta *Meus documentos* ou em suas subpastas, [illegible] banda larga. É bastante comum [illegible] encontrar computadores com [illegible] compartilhada. Se isso acontecer, você corre o [illegible] ter sua máquina invadida

Impressão em rede

Uma única impressora em sua rede é o suficiente para vários usuários. Basta compartilhar este dispositivo para que todos possam utilizá-lo através da rede

Windows

Para compartilhar uma impressora em sua rede, abra *Impressoras e aparelhos de fax* no *Painel de Controle*. Clique com o botão direito do mouse na impressora que deseja compartilhar e, em seguida, clique em *Compartilhamento*.

As opções exibidas na guia *Compartilhamento* podem ser diferentes dependendo do tipo de compartilhamento, ou seja, se ele está ativado ou não no computador. Para obter instruções sobre o que fazer em seguida, clique na opção que descreve o conteúdo da guia *Compartilhamento*.

Você precisa ativar o compartilhamento da impressora executando o *Assistente para configuração de rede*. Inicie o assistente clicando no link na guia *Compartilhamento* e siga as instruções. Quando o compartilhamento estiver ativado, inicie esse procedimento novamente. Você verá as opções para compartilhar ou não a impressora.

Na guia *Compartilhamento*, clique em *Compartilhar esta impressora* e digite um nome de compartilhamento. Se você compartilhar a impressora com usuários que utilizem outro hardware ou sistemas operacionais diferentes, clique em *Drivers adicionais*.

Selecione o ambiente e o sistema operacional dos outros computadores e, em seguida, dê *Ok* para instalar os drivers adicionais. Os drivers para usuários que executam outras versões do Windows (Windows 95, Windows 98 ou Windows NT 4.0) se encontram no CD de suporte desses sistemas. Os drivers de impressora para o Windows NT 3.1 e o Windows NT 3.5, porém, não estão incluídos.

Para finalizar, clique em *OK* ou, se tiver instalado drivers adicionais, clique em *Fechar*. Pronto, a impressora está compartilhada na rede.

Linux

Para que este compartilhamento funcione é necessário que a impressora esteja configurada e imprimindo sob o Linux e também que o servidor Samba esteja instalado. No arquivo *smb.conf* faça as seguintes mudanças:

```
[global]
printing = bsd
printcap name = /etc/printcap
load printers = yes
log file = /var/log/samba-log %m
lock directory = /var/lock/samba
[printers]
comment = Impressora Linux
security = server
path = /var/spool/lpd/lp
browseable = no
printable = yes
public = yes
writable = no
create mode = 0700
[ljet]
security = server
path = /var/spool/lpd/lp
printer name = lp
writable = yes
public = yes
printable = yes
print command = lpr -r -h -P %p %s
```

É muito importante que a rota para impressora (neste caso *[ljet]*) coincida com o diretório de tarefas temporárias em */etc/printcap*.

Na estação cliente você poderá encontrar a sua máquina Linux e a impressora compartilhada.

Dicas

Um servidor de impressão permite que você gerencie todos os documentos da impressora. Pode-se administrar todos os trabalhos que encontram na fila, alterar as prioridades dos documentos e mesmo cancelar impressões.

Mesmo que a impressora possua interface de rede, é ideal a utilização de uma estação para gerenciar a sua impressão, pois isso evita que usuários enviem documentos simultâneos provocando o surgimento de mensagens de erro.

Compartilhar conexão

Aprenda a configurar os servidores Windows e Linux para compartilhar o acesso de uma única conexão de banda larga com todos os usuários da sua rede

Windows

O Windows XP possui o recurso ICS (Internet Conection Sharing) instalado por padrão. Para configurar a aplicação, abra *Conexões de rede* no Painel de Controle. Clique com o botão direito do mouse sobre a conexao que você deseja compartilhar (Dial-up, Rede local ou PPPOE). No menu, selecione *Tarefas de rede* e em seguida em *Alterar as configurações desta conexão*.

Na guia *Avançado*, selec one *Permitir que outros usuários da rede se conectem pela conexão deste computador à Internet*. No caso de uma conexão Dial-up, selecione se deseja que a conexão seja efetuada automaticamente quando outro computador de sua rede tentar acessar recursos externos. Para isso, marque *Estabelecer uma conexão dial-up sempre que um computador da rede tentar acessar a Internet*.

Quando é ativado o compartilhamento de conexão com a Internet, o adaptador conectado à sua rede recebe uma nova configuração de endereço IP estático. As conexões TCP/IP existentes no computador que possui o compartilhamento de conexão com a Internet são perd das e precisam ser refeitas.

Para testar sua conexão de rede e com a Internet, vá a cada uma das estações de rede e execute o *Assistente para configuração de rede* a partir do CD do Windows XP desses computadores. Em seguida, verifique se é possível compart lhar arquivos entre os computadores e se cada máquina obtém acesso a um endereço na Web.

Depois que o ICS estiver ativado, certifique-se de que todos os computadores se comunicam entre si e têm acesso à Internet, como se estivessem conectados diretamente ao provedor de serviços de Internet. O compartilhamento de conexão deve ser usado em uma rede em que o computador host ICS controle a comunicação entre os computadores e a Internet.

Linux

Compartilhar sua conexão de banda larga usando o sistema Linux é bem simples. Com este serviço, computadores dentro da rede interna podem acessar simultaneamente um serviço HTTP (ou seja, navegar na Internet) e efetuar downloads de arquivos via FTP, utilizando um acesso à Internet.

O computador que faz o compartilhamento de conexão fará o papel de servidor NAT. Ele deverá possuir uma conexao com a sua rede local e também uma conexão de banda larga funcionando corretamente.

A versão atual é 2.4.x e possui recurso de implementar o servidor NAT de forma muito fáci com a utilização de recursos do *IPTABLE*. Com o editor de textos preferido abra o arquivo */etc/ rc.d/rc.local*. Neste arquivo, carregue o módu o NAT (mais todos os módulos dependentes) com o comando:

```
modprobe iptable_nat
```

Na tabela NAT (-t nat), adicione a regra (-A) após rotear (POSTROUTING) todos os pacotes encaminhados para fora via ppp0 (-o ppp0) e "mascarar" a conexão (-j MASQUERADE) no caso de interface rede tipo ADS_ trocar o ppp0 pelo dispositivo de rede (p.ex. eth0):

```
iptables -t nat -A POSTROUTING -o ppp0 -j
MASQUERADE
```

Habilite o encaminhamento dos pacotes:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Após adicionar as linhas seguintes no arquivo, reinicie seu servidor para que as alterações tenham efeito. Ao ligar novamente o computador, o sistema já estará funcionado corretamente

Dicas

Compartilhar uma conexão Internet significa que a estação que está executando a tarefa pode ser encontrada pelos usuários da Internet. Portanto há riscos que ataques sejam realizados. É recomendável que se utilize firewall e evite compartilhar documentos nestas estações, já que existe a possibilidade de serem copiados por usuários mal-intencionados.

Na página 34 você encontra uma reportagem com as várias falhas de vulnerabilidades que podem existir em uma rede.

Acesso remoto

Administre seu computador a distância. Do seu escritório é possível se conectar e exibir o Desktop de sua estação para realizar todo o trabalho como se estivesse no local

Windows

O Windows XP possui um recurso nativo, a Area de Trabalho Remota, que permite que se tenha acesso ao desktop remotamente. Pela primeira vez a Microsoft disponibiliza esse aplicativo aos usuários domésticos. Até então, este tipo de acesso remoto só estava disponível na linha de servidores Windows 2000, onde é chamado de Terminal Service.

Preparando o servidor

No Windows XP, abra o *Sistema* no *Painel de Controle*. Na guia *Remoto*, marque a caixa de seleção *Permitir que usuários se conectem remotamente a este computador* e clique em *OK*.

Na janela, certifique-se de ter as permissões adequadas para se conectar remotamente ao seu computador e clique em *OK*. Você deve ser um administrador ou um membro do grupo *Usuários* da área de trabalho remota no seu computador.

Na estação remota

No computador que executa o Windows 95, Windows 98, Windows NT ou Windows 2000, insira o CD do Windows XP na unidade de CD-ROM.

Quando a página de boas-vindas aparecer, clique em *Executar tarefas adicionais* e, em seguida, clique em *Configurar a conexão com uma área de trabalho remota*. Siga as instruções na tela.

Após esta operação, o software cliente já estará instalado. Carregue o aplicativo que se encontra no menu *Iniciar* e informe o endereço IP do computador que se deseja conectar.

Este recurso de acesso remoto não permite que a estação que possui o Windows XP esteja sendo usado no momento da conexão. O sistema exibirá uma mensagem e apagará o sinal do monitor durante a conexão.

Linux

Para o Linux, a solução para fazer acesso remoto é o VNC (Virtual Network Computing). Com ele, você pode acessar seu computador de qualquer lugar usando um navegador Internet que tenha suporte a Java. Você encontra o VNC no endereço www.uk.research.att.com/vnc/dist/. Para realizar sua instalação, faça o download do programa e copie para o diretório raiz de seu computador. Descompacte utilizando o comando:

```
# tar -zxvf vnc-XXXX_linux_2.0.tgz
```

Entre na pasta onde os arquivos foram descompactados:

```
# cd vnc_x86_linux_2.0
```

Dentro da pasta, copie os arquivos para a pasta de executáveis. Digite o comando:

```
# cp vncviewer vncserver vncpasswd
vncconnect Xvnc /usr/local/bin
```

Ainda dentro da pasta, digite o comando:

```
# mkdir -p /usr/local/vnc/classes
```

Copie os arquivos executando o comando:

```
# cp classes/* /usr/local/vnc/classes
```

Para inicializar o servidor no sistema VNC, digite:

```
# vncserver
```

Após digitar o comando acima, o programa irá solicitar uma senha para restringir o acesso de pessoas não autorizadas. Para acessar o Linux de um outro computador, abra o Browser e digite o seguinte endereço http://endereço_do_ip:5801, onde *endereço do IP* é o IP do servidor VNC. Sempre que iniciar um novo servidor utilizando o comando *vncserver*, será aberto um novo servidor e o anterior será mantido.

O VNC pode ser obtido para várias plataformas como Windows 9x, NT e 2000, sendo uma ótima opção para os usuários que não possuem o Terminal Service

Dicas

Utilize senhas fortes. Ao se criar este tipo de recurso em sua conexão de rede o risco de invasão pode ser grande, e a única forma de se evitar problemas com este tipo de conexão é a senha, portanto evite senhas simples como o seu nome ou o nome do computador. O uso de senhas fracas está entre as 10 maiores falhas segundo o FBI (veja na página 6).

Este recurso pode ser muito útil para executar tarefas remotamente, como obter documentos ou mesmo realizar trabalhos de manutenção. É uma ótima solução para quem realiza suporte.

Proxy descomplicado

O Proxy pode ser muito útil para redes, já que permite criar um cache das páginas visitadas no servidor e pode ser usado para compartilhar a conexão Internet

Windows

O Windows não possui nenhum software nativo por padrão que execute a tarefa de Proxy. A solução é utilizar alguma aplicação desenvolvida por terceiros. Um dos softwares mais famosos, adotado com freqüência, é o Wingate (www.deerfield.com). Trata-se de um software comercial, mas pode ser usado livremente por 30 dias.

Para que este software funcione é necessário que sua rede esteja rodando corretamente o protocolo TCP/IP. Faça em seguida o download do software

Com o software em seu computador, faça a instalação do mesmo. Execute o programa que você baixou da Internet. Isto fará com que o Wingate, o utilitário cliente GateKeeper e os arquivos de ajuda sejam instalados no diretório *C:\Arquivos de Programas\Wingate*, ou outro a ser escolhido por você na hora da instalação

Na estação cliente, localize no servidor que você acabou de instalar o aplicativo *If you are installing from an installation file downloaded from the Internet, locate the file wg3059x.exe* (para Windows 9x) ou *wg305nt.exe* (para Windows NT). Copie o arquivo para a estação e dê um duplo clique no arquivo para iniciar o processo de instalação.

Siga as instruções das telas para continuar a instalação. O processo de instalação irá detectar o servidor WinGate operando na rede e, por padrão, irá passar para a instalação do Cliente Wingate.

O monitor do WinGate Engine inclui um ícone no *Systray* do Windows que fornece uma indicação visual se ele está rodando ou não. Você pode acessar rapidamente o GateKeeper dando um duplo clique neste ícone.

O Wingate permite que as estações clientes naveguem na Internet apenas com a instalação do software, sem a necessidade de configuração de Proxy no Browser

Linux

O servidor Proxy Squid pode melhorar a velocidade de navegação na Web por meio do recurso de cache de memória e disco. O Squid mantém na memória e no disco as páginas, imagens e arquivos transferidos dos sites. Caso dois ou mais usuários acessem o mesmo site um após o outro, o segundo e subsequentes vão notar que a página carrega muito rapidamente, pois na verdade a página está sendo entregue diretamente da memória cache ou cache de disco, em vez de ser solicitado ao site novamente.

O primeiro passo é instalar o Squid. A distribuição Mandrake desta edição traz o software, basta instalar através do Control Center (veja matéria na página 44).

Edite o arquivo de configuração */etc/squid/squid.conf*. Descomente a linha referente a porta padrão do Squid e a linha referente ao cache de RAM, que pode ser alterada conforme disponibilidade de RAM. Descomente a linha:

```
cache_dir ufs /var/spool/squid 100 16 256
```

Edite os parâmetros do cache de disco. Uma vez configurado conforme acima, execute a inicialização da área de cache em disco.

```
#] squid -z
```

Execute o serviço Squid. Em Linux com suporte a arquivos de inicialização de serviços tipo System V, pode-se digitar:

```
#] service squid start
```

Ou simplesmente.

```
#] squid
```

Para execução automática do serviço habilite com comando ntsysv e selecione o Squid, ou edite o arquivo de inicialização /etc/rc.d/rc.local para que o Squid seja executado durante a inicialização.

Nas estações clientes configure o navegador Web para a utilização do servidor proxy Squid, basta preencher as informações do seu servidor no proxy.

Dicas

O uso de proxy possui um maior controle dos usuários que utilizam a conexão Internet. Permitindo levantar o relatório das páginas visitadas.

Além dos relatórios, o Proxy permite controlar o acesso de usuários a sites que podem ter conteúdo inadequado ao ambiente de trabalho, bloqueando a exibição da página.

Também é possível restringir o acesso a certas páginas por horário. Com isso, pode-se por exemplo, não permitir acesso a páginas de piadas durante o período de trabalho.

Delphi 7 Studio

A nova versão do principal ambiente de desenvolvimento da Borland está ainda mais voltada para a Internet

Por Leandro Calçada
leandro.calcada@europanet.com.br

Muito mais uma evolução do que uma revolução. O Delphi 7 Studio, a mais nova plataforma de desenvolvimento da Borland, não trouxe nenhuma novidade realmente revolucionária entre seus componentes e ferramentas de desenvolvimento, mas reforçou e ampliou as novas propostas de desenvolvimento estabelecidas com o Delphi 6.

Estas propostas, entretanto, têm mostrado que a Borland, com intensidade crescente, aposta mais nos desenvolvedores de aplicações para rede e menos no desktop. Confira as principais novidades do Delphi 7 Studio e veja se vale a pena a atualização.

Rumo à Web

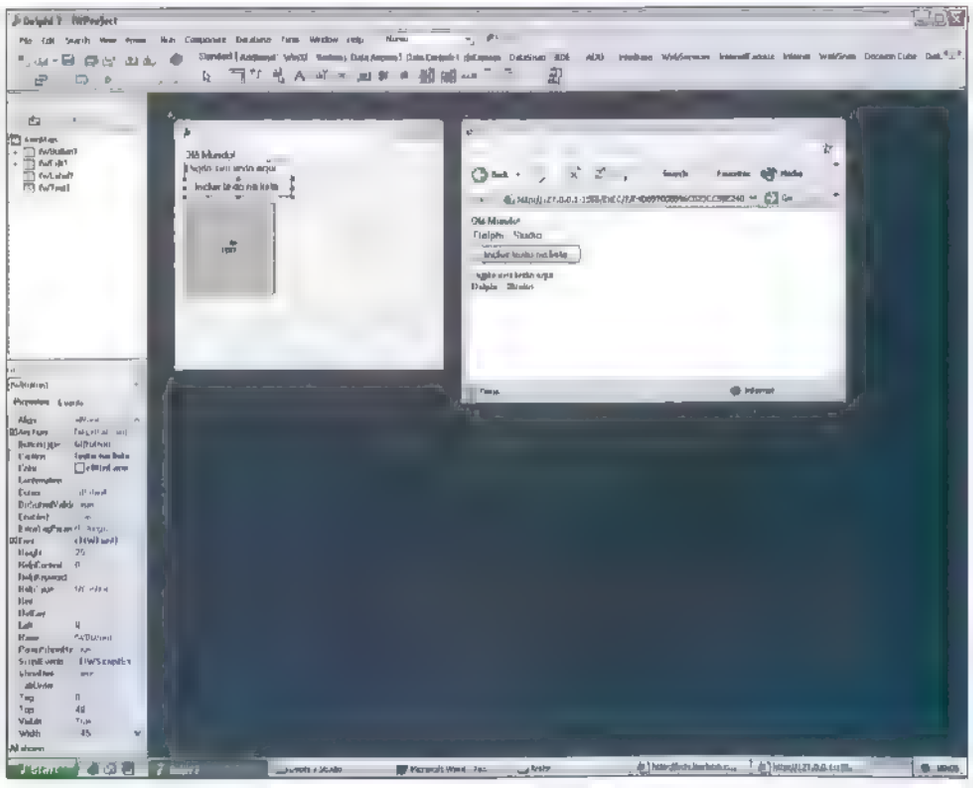
O suporte a desenvolvimento de Webservices, iniciado com o Delphi 6, foi fortalecido no Delphi 7 Studio e agora é fornecido em todas as versões, com exceção da versão Personal. Classes foram adicionadas aos componentes SOAP, permitindo um controle mais eficaz da comunicação entre as aplicações Delphi e seus servidores ou clientes, através de SOAP e XML.

Também ficou mais robusto o suporte à plataforma de servidores Web Apache. Com o Delphi 7, é possível criar Webservices também para Apache 2, sem o uso de componentes adicionais. Por outro lado, o suporte a WinCGI implementado no Delphi 6, apesar de ainda disponível, já não é recomendado aos desenvolvedores, e provavelmente será descontinuado já na próxima versão do Delphi.

Mas a maior inovação para quem desenvolve para a Internet com o Delphi, foi a adição dos componentes IntraWeb. Com eles é possível criar aplicações para o Apache, com a mesma simplicidade com que se desenvolve aplicações desktop. Com estes componentes, é possível desenhar formulários visualmente, criar toda a lógica da aplicação Web em Object Pascal e, após compilado o projeto, testá-lo localmente com um pequeno servidor que já vem no Delphi, ou ainda utilizar a aplicação diretamente em Apache 1 ou 2, sem se preocupar com códigos HTML ou scripts Java.

Bases de Dados

O suporte à Borland Database Engine ainda existe mas seu uso é cada vez mais desencorajado pela Borland. Em seu lugar há o suporte a bases de dados ADO, Interbase, e os componentes dbExpress, introduzidos a partir do Delphi 6 e que, apesar de bem limitados, são capazes de oferecer



Com os componentes IntraWeb ficou mais fácil criar aplicações para o Apache

suporte a dados a uma aplicação Delph com o menor overhead possivel.

Como a maioria dos componentes, o suporte a bancos de dados do Delphi 7 é uma evolução da ideologia implantada no Delphi 6. Os objetos de DataSnap, por exemplo, sofreram mudanças apenas para corrigir pequenas falhas de projeto da versão do componente para o Delphi 6.

Já o suporte a servidores SQL fo transferido definitivamente para os componentes dbExpress, que continuam oferecendo suporte apenas unidirecional a bases SQL, ou seja, sem cache automático. Por outro ado, estes componentes continuam 100% compatíveis com os componentes dbExpress do Kylix, permitindo o desenvo vimento mu tip ataforma sem que uma linha de código seja reescrita.

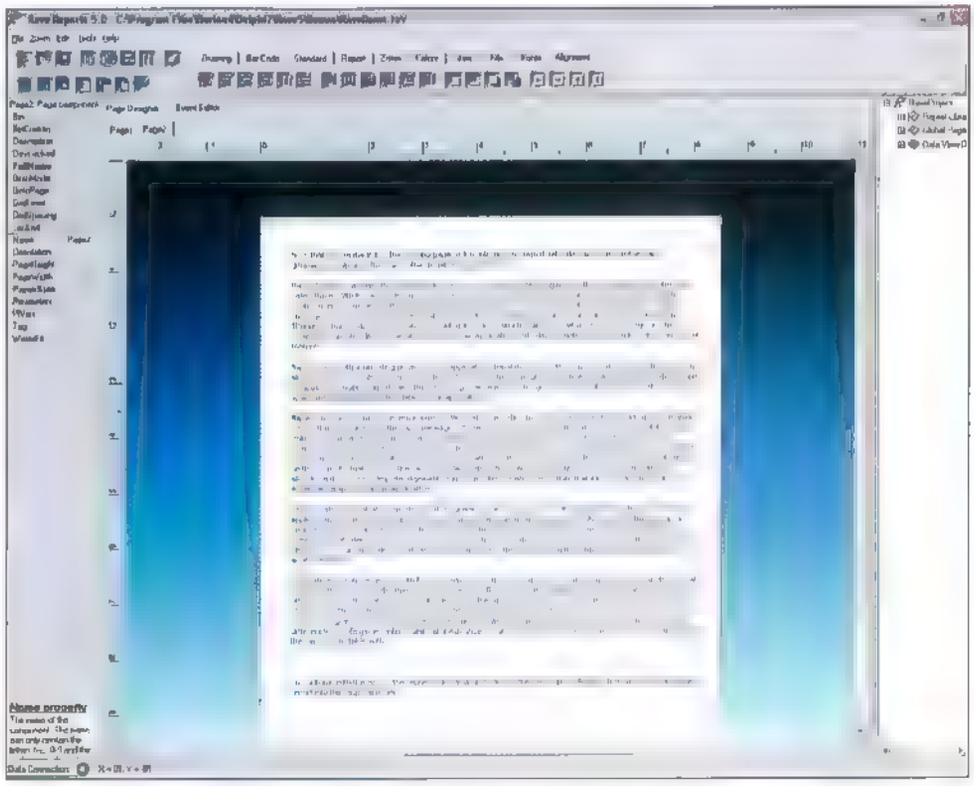
Poucas mudanças na CLX

Assim como no Delphi 6, é possível desenvolver aplicações específicas para Windows com a VCL, ou utilizar a CLX (Biblioteca de Componentes Multiplataforma), e desenvolver aplicações para ambas as plataformas com um único código-fonte. Para a CLX propriamente dita, que foi uma das grandes revoluções do Delphi 6 e que ainda precisa de muitos recursos adicionais, tudo o que a Borland reservou foi a criação de uma aba System específica, com alguns componentes para a manipu ação visual de arquivos, e algumas pequenas atualizações nas caixas de diálogo padrão. Uma melhora muito pequena para valer uma atualização.

Adeus ao QuickReport

Se não há grandes novidades para quem usa a CLX, aos usuários do QuickReport está reservado um verdade.ro choque. Não há mais QuickReport. O sistema, que sempre foi pesado e cheio de vazamentos de memória, precisava ser substituído há muito tempo mas, talvez até por uma questão de custo de licenciamento, a Borland não optou por uma substituição gradual e eliminou o QuickReport, substituindo-o pelo Rave Reports.

Entretanto, o Rave Reports trabalha de uma forma completamente diferente do QuickReport, e exige do usuário deste serviço uma curva de aprendizado alta. A adoção de um componente de relatórios mais leve, e que também funciona no Kylix é certamente um grande progresso, mas uma transição leve, como a que vem sendo fe.ta com os usuários da outrora consagrada BDE, certamente não desagradaria ninguém.



O editor de relatórios do Rave Reports é simples, intuitivo e pode ser usado no Kylix

Como pontos positivos do Rave Reports, convém ressaltar o editor de páginas de relatório, completamente separado da IDE e muito mais amigável para quem não está acostumado com estas ferramentas, e a capacidade de seus componentes, de exportar os re atórios em formatos como HTML e PDF com extrema facilidade.

Considerações Finais

O Delphi 7 Studio traz algumas novidades e mu tos aperfeiçoamentos mas traz, também, pequenos problemas recorrentes e que parecem totalmente abandonados pela Borland. O suporte a imagens JPEG, por exemplo, apresenta um vazamento de memória desde que foi implementado, na versão 3 do Delphi, e que ainda não foi corrigido. O sistema de ajuda, que sempre teve uma forte ligação entre os tópicos de ajuda e os componentes da IDE, está cada vez mais comp exo, isso sem falar nos componentes cuja ajuda não existe ou, quando existe, não está apropriadamente ligada ao ambiente de desenvolvimento.

Vale a atualização? Depende: se você está com uma versão 5 ou anterior do Delphi, e quer desenvolvimento multiplataforma Windows/Linux em Object Pasca , ou se compatibilidade com .NET e desenvolv mento para Apache são essenciais, então faça a atual zação. Por outro lado, se o seu alvo principal é desenvolvimento de aplicações .ocais para desktop ou bases de dados baseadas na BDE, então f que com a sua versão atual do De phi. **PCM**

Kylix 3

Desenvolva aplicações para Linux rapidamente usando Object Pascal ou C++

Por Leandro Calçada
eandro.calcada@europanet.com.br

Já na terceira versão, o Kylix é a ferramenta mais fácil de usar para quem está migrando do Windows e procura um ambiente integrado de desenvolvimento para Linux. Baseado em uma estrutura de componentes similar à do Delphi e do C++ Builder, o Kylix é até agora o mais próximo que se pode chegar da programação multiplataforma entre Windows e Linux, sem o uso de Virtual Machines ou Frameworks de qualquer tipo. Se você é um desenvolvedor que usa os produtos da Borland, e quer oferecer soluções baseadas em Linux, esta pode ser a sua chance.

Mais do mesmo

Ao contrário do Delphi 7, que trouxe poucas novidades, aos usuários do Kylix a Borland reservou muitas surpresas para o ambiente de desenvolvimento. A IDE, que nas duas versões anteriores do Kylix era pesada e limitada, agora inclui praticamente todos os recursos das IDEs das últimas versões do Delphi e do C++ Builder. Se para o desenvolvedor Windows estas novidades não são exatamente novas, para quem já se debateu com o Kylix 1 e 2, ter à mão recursos como o TreeView ou a página de Diagramas pode ser exatamente o alívio que faltava para tocar o desenvolvimento em Linux de forma mais organizada.

Também foram atualizadas a barra de componentes, que se comporta agora da mesma maneira que nas versões Windows das IDEs da Borland, e o CodeInsight. Este último, uma espécie de Auto Completar, foi criado para ajudar os desenvolvedores com as extensas listas de propriedades e métodos usadas na programação orientada a objeto, mas já estava ficando cada vez mais pesado e lento. Com a atualização, tanto o CodeInsight do Delphi 7, quanto o do Kylix, ficaram um pouco mais leves e rápidos, um recurso que sempre agrada quem não tem tempo algum a perder.

Multiplataforma e Multilinguagem

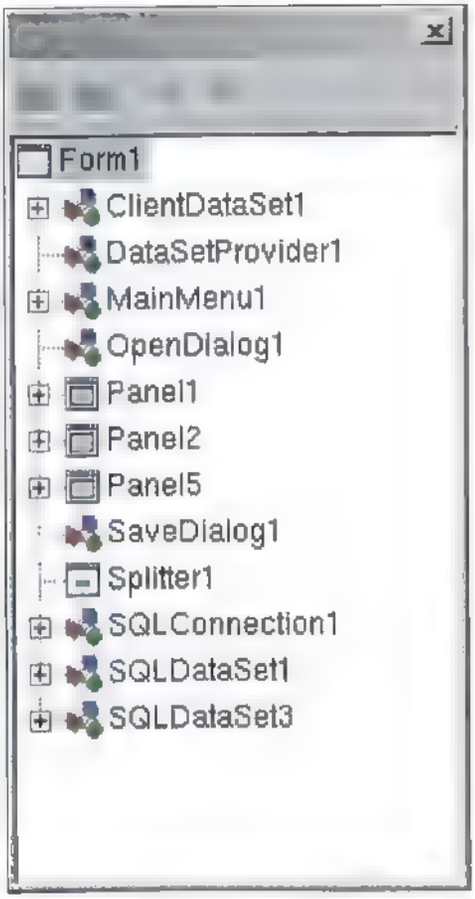
Além de possibilitar o desenvolvimento em Windows e Linux, sem mudanças no código, o Kylix 3 trouxe também a possibilidade de escolha da linguagem de programação usada na IDE. Enquanto em Windows, o Delphi – no qual se desenvolve em Object Pascal – e o C++ Builder – no qual se desenvolve em C++ – são produtos separados (apesar de compartilharem IDEs e componentes semelhantes) no Kylix ambos são parte de um só produto. Iniciando o Kylix em C++ Mode obtém-se um ambiente gráfico de desenvolvimento para programar em C++ no Linux. Já ao iniciar Kylix em Delphi Mode, obtém-se o mesmo ambiente gráfico, mas com suporte a Object Pascal.

E esta não é a única novidade. Mesmo sendo duas IDEs distintas cada qual capaz de criar formulários e units na sua própria linguagem, ambas podem usar o código uma da outra, sem quaisquer alterações. Isso significa que um usuário habituado a usar o C++, pode desenvolver no Kylix C++ e ainda assim fazer uso das funções, formulários e componentes criados por seu companheiro que usa o Kylix Delphi e programa em Object Pascal.

A CLX e o Linux

Quando foi lançado, o Kylix inaugurou uma nova filosofia para a Borland. A filosofia do desenvolvimento multiplataforma. Para atingir este objetivo, entretanto, não basta criar uma IDE para outro sistema operacional, tarefa que, aliás, a Borland parece só ter concluído agora. É preciso também ter componentes e funções que funcionem da mesma forma em ambas as plataformas.

Para isso, foi criada a CLX, um



O TreeView, que facilita a organização dos componentes de um formulário, agora está no Kylix também

conjunto de componentes e bibliotecas único capaz de funcionar adequadamente tanto em Windows quanto em Linux, sem exigir mudanças na programação, ao menos em teoria.

Na prática, porém, a CLX parece nunca estar totalmente adaptada ao Linux. Diversas propriedades de seus componentes, principalmente do próprio formulário, que funcionam de forma perfeita no Windows, simplesmente não funcionam no Linux, ou funcionam de modo irregular.

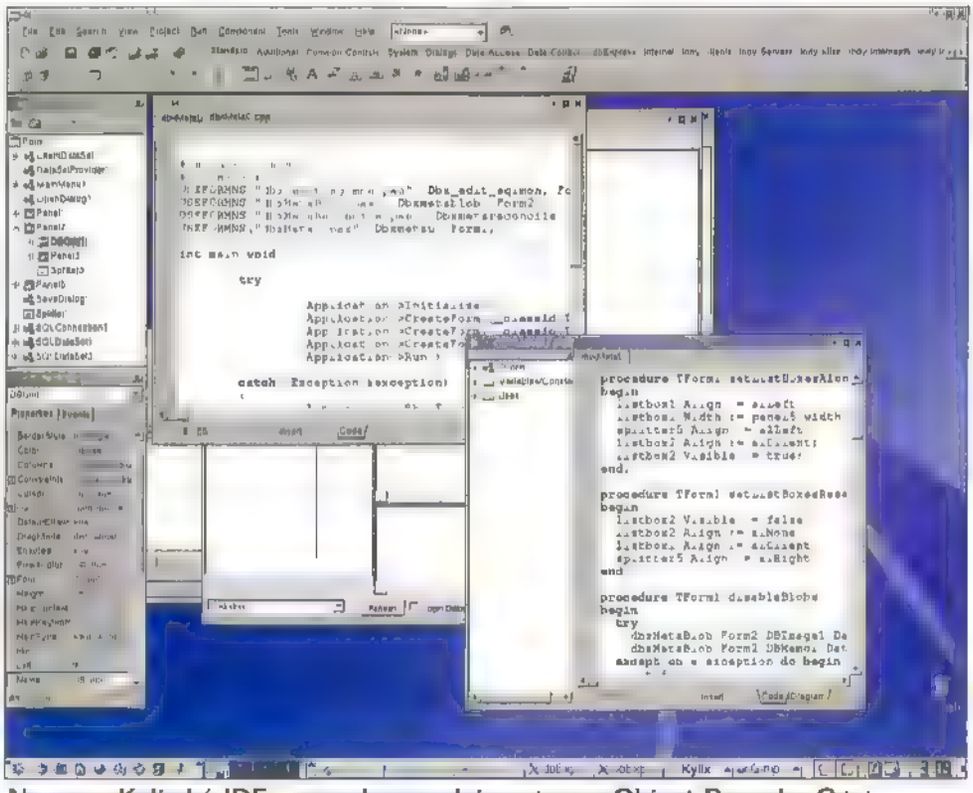
Isso acontece principalmente porque, no Linux, há muitos gerenciadores de janelas diferentes, cada qual com o seu comportamento específico, o que afeta drasticamente o comportamento de itens básicos como botões e bordas de janelas.

Mesmo não sendo um problema de responsabilidade direta da Borland, estas pequenas incompatibilidades da CLX dificultam ou mesmo invalidam completamente um projeto multitarefa, dependendo de quais forem os requisitos fundamentais de funcionamento do programa a ser desenvolvido.

E há ainda o problema das poucas novidades. Por ser uma biblioteca de componentes relativamente nova, esperava-se que a CLX demonstrasse uma grande evolução entre estas primeiras versões do Kylix, mas tudo o que se viu foi a mera adição de alguns pequenos componentes para a visualização de arquivos. Se por um lado os componentes são muito práticos e bem construídos, por outro não são suficientes para que se possa dizer que a CLX está cheia de novidades.

WineLib e Outros Bichos

Apesar de bastante evoluída, a IDE do Kylix 3 ainda sofre de um problema muito sério. Sua dependência da WineLib. A WineLib é um conjunto de bibliotecas do Wine que permite executar funções muito semelhantes às das APIs básicas do Windows, no Linux. Este recurso foi essencial para que a IDE do Delphi 5, na época, pudesse se transformar no ambiente de desenvolvimento do Kylix 1, mas esperava-se que a WineLib fosse abandonada com o tempo, pois, apesar das facilidades, ela só aumenta o overhead causado pela IDE.



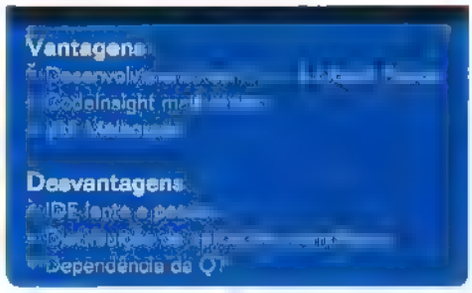
No novo Kylix há IDEs para desenvolvimento em Object Pascal e C++

Outro problema do Kylix 1 e 2 que ainda não foi resolvido, é a dependência de bibliotecas específicas. Ao contrário do Delphi e do C++ Builder, que são capazes de gerar executáveis completos distribuídos sem nenhuma biblioteca adicional, o Kylix, além de depender das bibliotecas QT, que são a base do KDE, ainda depende de uma série de bibliotecas específicas da própria Borland. Essas bibliotecas devem ser instaladas no sistema alvo antes que qualquer aplicação Kylix possa rodar.

É fácil perceber o quanto isso pode complicar a vida de um usuário: basta lembrar que a instalação do Kylix não liga estas bibliotecas ao sistema operacional, de modo que o próprio desenvolvedor, se não instalar as bibliotecas manualmente, jamais conseguirá rodar seus programas fora da IDE.

Considerações Finais

Se as mudanças na CLX são essenciais para você, ou se for impossível sobreviver sem as novidades na IDE, então atualizar o Kylix para a versão 3 é uma tarefa obrigatória. O mesmo pode ser dito aos desenvolvedores C++ que não estiverem dispostos a se aventurar no estranho e fascinante mundo ASCII do Emacs e do gcc. Por outro lado, se o Kylix 1 ou 2 já atende às suas necessidades e tudo que você esperava era que a IDE ficasse mais leve, ou que as complicações de distribuição fossem solucionadas, o melhor é ficar longe do Kylix 3. **PCM**



Mac sabor U

Testamos a nova versão do Mac OS X, um sistema com muitos dos recursos que existiam apenas em Unix, agora disponíveis para os computadores Apple

A Apple acaba de lançar o Jaguar, a mais nova versão do seu sistema operacional, o Mac OS X v 10.2. Com muitos avanços, o novo sistema apresenta boas melhorias em relação à versão anterior.

O projeto do sistema operacional da série X tem o kernel Darwin, baseado em um modelo de Unix, que tem como principal característica o seu código aberto. Isso permite que desenvolvedores voluntários ajudem no seu aperfeiçoamento. Com isso, além de comandos semelhantes, o sistema operacional da Apple tem o apoio de toda a comunidade Unix.

Com o kernel baseado em Unix, o novo modelo de sistema operacional tornou-se multitarefa, o que permite realizar trabalhos complexos, como renderização de imagens ou compressão de vídeo, que exigem muita capacidade de processamento. Agora, o kernel organiza a prioridade das tarefas, distribuindo os recursos necessários para que você não tenha de esperar enquanto o computador está processando.

Outro ponto que merece destaque é a implementação total do protocolo TCP/IP. Isto já era previsto, uma vez que se trata de um sistema operacional baseado no Unix. Mas a compatibilidade com a rede Apple Talk foi 100% mantida.

Vale mencionar também que agora há uma versão do servidor Web Apache no sistema operacional. Desta forma, é possível, com simples configurações, compartilhar arquivos e sites através da sua rede local ou da Internet.

Para finalizar, também é possível usar dois formatos de partições para armazenar seus dados: o HFS+, que já era o padrão dos Macintoshs, e o UFS (Unix File System). Este último é o padrão da maioria dos sistemas baseados no Unix.

Interface gráfica

Um dos pontos fortes no Mac OS X é sua interface gráfica. O sistema operacional possui um servidor, Quartz, muito semelhante ao XFree86. Ele processa os dados e depois os envia para um gerenciador de janelas, o Aqua, que é também semelhante aos gerenciadores de janela do Linux.

O Aqua é um ambiente bastante amigável e, principalmente, veloz. Mas o mais importante mesmo é o servidor do modo gráfico Quartz.

Este software utiliza uma técnica que, ao contrário de outros sistemas operacionais, não exibe mais imagens no formato bitmap. No Mac OS X, todas as imagens que aparecem na tela são vetoriais e são processadas pelo servidor no formato PDF.

Aliás, praticamente tudo o que o Mac OS X faz utiliza a tecnologia PDF. Ao solicitar um preview de impressão, por exemplo, uma imagem do documento é convertida para o padrão PDF e os resultados são apresentados na tela do usuário de uma forma bem mais rápida. Mas não pense que somente os usuários finais poderão se beneficiar deste recurso. Os componentes também passaram a ser vetoriais, facilitando muito a criação de interfaces de aplicações para os desenvolvedores.

Assim como nas versões anteriores do Mac OS, o menu continua sendo apresentado na parte superior da tela. A novidade está mesmo na parte inferior, onde foi adicionada uma espécie de barra de tarefas chamada Dock.

O Dock, porém, vai muito além de uma simples barra de ferramenta. Este recurso permite arrastar atalhos para aplicativos e até mesmo visualizar um preview de uma imagem que está minimizada. Vale destacar um interessante efeito especial que aparece cada vez que você minimiza uma janela: a impressão que se tem é que ela está sendo sugada pelo Dock.

nix

Um outro recurso adicionado nesta versão do Mac é o Inkwell. Usando uma mesa digitalizadora o sistema é capaz de reconhecer a escrita feita no dispositivo e carregá-la para qualquer aplicativo que esteja sendo usado.

Compartilhamento

Compartilhar arquivos com outros computadores ficou mais fácil com esta nova versão pois foram adicionados diversos aplicativos de compartilhamento. Um bom exemplo é o Apache, um dos mais famosos servidores Web. Este software já vem instalado como padrão, na versão 1.3. Para ativá-lo, basta carregar o System Preferences que está localizado no Dock, clicar sobre a opção Sharing e marcar o item Web Sharing On. A partir daí a utilização do programa segue exatamente igual as versões que já existiam para Linux ou Windows.

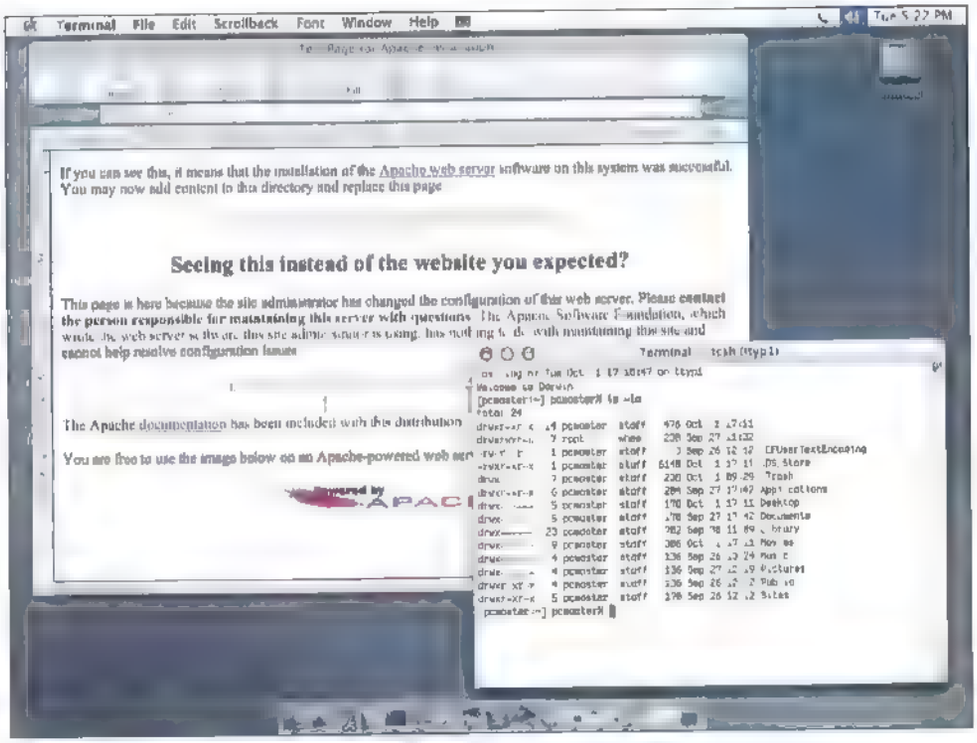
Além do Apache, outro recurso bastante comum para compartilhar o conteúdo de seu computador na Internet é o FTP, que também está presente neste sistema. Com esse aplicativo você pode se conectar ao seu computador através de um terminal SSH. Para os usuários de sistemas Unix este recurso já é bem conhecido, pois abre um terminal Unix remotamente.

Se o seu computador estiver conectado a uma rede com estações Windows, pode-se compartilhar e conectar arquivos e diretórios como se fosse uma estação Windows.

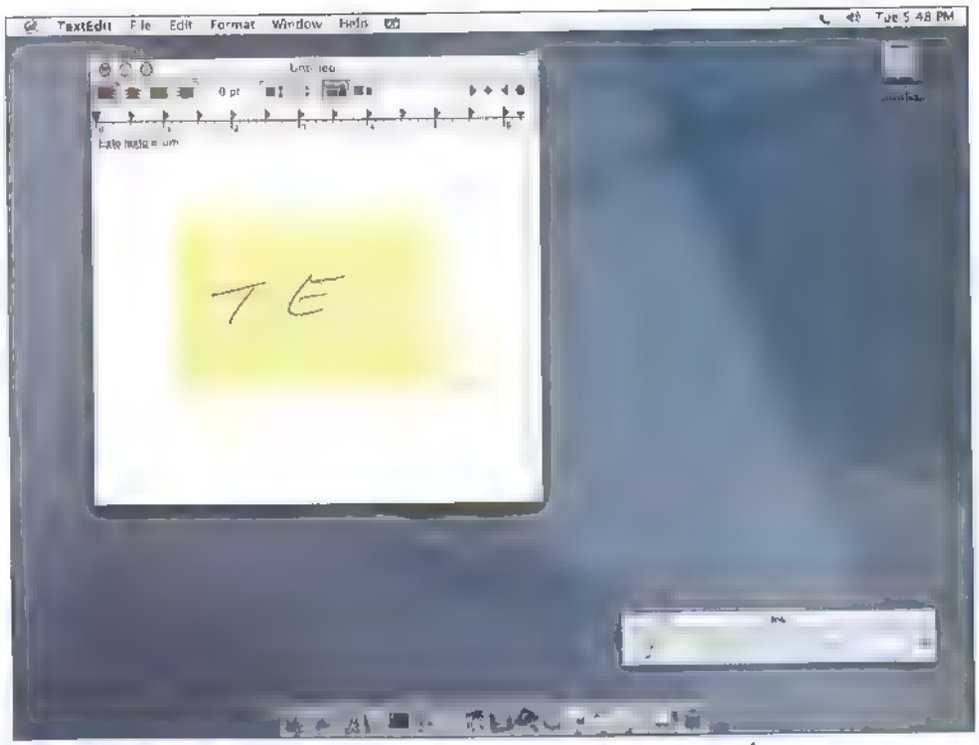
Conclusões

Com os testes feitos nesta nova versão do Mac OS X podemos destacar entre suas principais qualidades, o ambiente gráfico, ideal para iniciantes e eficiente para usuários avançados. Há ferramentas bastante úteis como por exemplo, um software de configuração de rede e o servidor Apache, também um terminal shell para os usuários que estão habituados ao Linux e Unix.

Porém, um problema que pode fazer com que este sistema operacional não se popularize é o alto custo dos computadores da linha Macintosh, que aqui no Brasil são vendidos por cerca de R$ 8.000,00, um preço bastante elevado em comparação com os PCs. **PCM**



Ao se olhar pela primeira vez o Mac OS X pode ser confundido com uma estação Unix, já que possui terminal shell e servidores Web Apache (acima), FTP e SSH



O Inkwell permite reconhecer a escrita. Basta conectar ao computador uma mesa digitalizadora, abrir o software e escrever para que o texto seja carregado

BugBear

Quando todos achavam que o vírus mais perigoso de 2002 seria o Klez surgiu uma nova praga. Saiba como funciona o BugBear e porque o pânico em torno dele não é alarmismo

Por Leandro Calçada
leandro.calcada@europanet.com.br

O ano de 2002 tinha tudo para ser tranquilo. Apesar dos novos vermes e vírus desenvolvidos a cada dia, a praga mais perigosa datava de abril, e ainda respondia pelo nome de Klez. Analistas de segurança do mundo inteiro já comemoravam o fato de que este ano estava definitivamente mais calmo que os anteriores e houve até quem previsse, mais uma vez, o fim desta forma de ataque a nossos computadores.

Mas tudo o que é bom acaba, e antes que 2002 pudesse ser comemorado, surgiu um novo vírus, com uma capacidade de infecção tão alta quanto a do Klez e uma capacidade de destruição ainda maior: o BugBear

Ficha Técnica

Nome do vírus: BugBear
Plataforma: Win32/NT
Descoberto em: 30/09/2002
Tamanho: 50 688 ou 50 664 bytes
Capacidade de reprodução: Alta
Risco: Alto
Sistema-Alvo: Windows 95/98/ME/NT/2000/XP
Apelidos conhecidos:
W32/Bugbear@MM (NAI)
W32 Bugbear@mm (Symantec)
W32/Bugbear-A (Sophos)
W32/Bugbear.A@mm (F-Secure)
Win32.Bugbear (CA)
Worm/Tanatos (CentralCommand)
WORM_NATOSTA.A (Trend)

Distribuição

Assim como o Klez, o BugBear distribui-se por e-mail ou pela rede Windows. Quando enviado por e-mail, o vírus procura explorar falhas de segurança no Internet Explorer que permitem que um anexo seja executado automaticamente quando a mensagem é aberta no Microsoft Outlook ou no Outlook Express. Além disso, como já virou tradição entre esta categoria de vírus, o e-mail traz textos, no assunto e no corpo da mensagem, que estimulam o usuário a abrir o anexo espontaneamente, garantindo a infecção mesmo que não haja falhas de segurança em seu cliente de e-mail.

É importante ressaltar que o vírus possui seu próprio cliente de SMTP e é capaz de localizar o servidor SMTP do usuário infectado através de buscas no Registro do Windows. Além disso, o vírus procura endereços de e-mail para infectar não só no Catálogo de Endereços do Windows, mas também em arquivos de e-mail de diversos formatos. Conclusão: até quem não usa o Outlook Express pode servir como foco de infecção por e-mail.

Já ao se espalhar pela rede Windows, o BugBear cria cópias de si mesmo em qualquer pasta compartilhada que tenha acesso de escrita, esteja ela protegida por senha ou não. E se o BugBear encontrar o disco de sistema compartilhado, um erro que muitos usuários iniciantes cometem em suas redes locais, o vírus criará uma cópia de si mesmo na pasta de inicialização do sistema, garantindo a infecção mesmo que o usuário não execute nenhum arquivo.

Ao ser executado, o BugBear assume o comportamento padrão dos vermes e vírus de e-mail modernos: copia-se para as pastas de sistema, cria chaves de registro para se executar automaticamente a cada boot e ativa a sua carga destrutiva imediatamente.

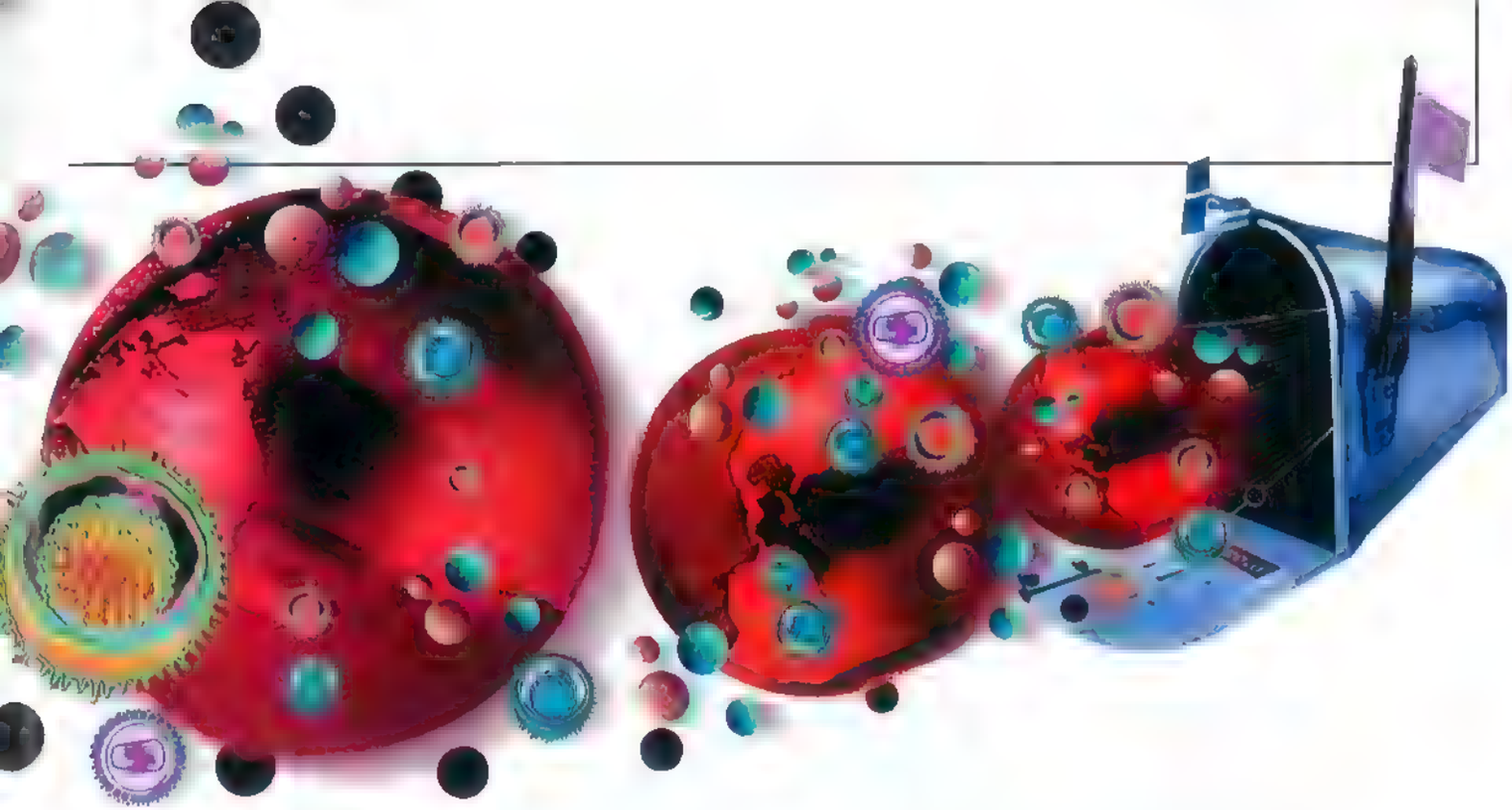
A arte do convencimento

Caso as falhas de segurança do Internet Explorer não ajudem, é

Como se defender

Mantenha sempre o seu antivírus atualizado e, caso esteja usando o Internet Explorer 4 ou 5, faça todas as atualizações de segurança da Microsoft, pois só assim é possível evitar que o vírus rode automaticamente ao ser aberto um e-mail infectado no Outlook Express.

Mesmo sem as vulnerabilidades é preciso tomar cuidado com arquivos anexos de origem suspeita, mesmo que venham de e-mails aparentemente familiares. E como o vírus é capaz de espalhar-se através da rede Windows é de extrema importância não deixar nenhum compartilhamento de pasta completo (com acesso à escrita), mesmo que com senha, pois é através destes compartilhamentos que o BugBear se espalha pela rede local



preciso convencer o usuário atacado pelo BugBear, a abrir o arquivo anexo ao e-mail, para se infectar. Para atingir este objetivo o BugBear, assim como seus semelhantes, tem os seus truques. Além do velho truque do arquivo com extensão dupla, lançado pelo I Love You, o vírus pode usar, como nome do anexo, o nome de algum dos arquivos do computador originalmente infectado.

E como se não bastasse, o BugBear pode falsificar o endereço do remetente, montando nomes e e-mails com os dados coletados na máquina do usuário infectado. Funciona assim: se um usuário infectado tem em seu Catálogo de Endereços o usuário Antonio Ferreira, com o e-mail *antonio@provedor.com.br* e o usuário Joao Santos, com o e-mail *joao@minhacasa.com.br*, o BugBear pode enviar-se em uma mensagem para um deles em nome de Antonio Santos, usando o e-mail *antonio@minhacasa.com.br*

Portanto, se você receber um e-mail do seu melhor amigo com um arquivo anexo desconfie. Os "computadores-zumbis" estão por toda parte.

Capacidade de Destruição

O vírus não apaga arquivos, nem destrói o sistema operacional, mas faz algo ainda pior. Ao infectar um computador, a primeira tarefa que o BugBear assume é a de desligar qualquer antivírus ou firewall que ele reconhecer, a começar pelas ferramentas mais famosas do mercado – e que a maioria dos usuários utiliza.

Desligadas as ferramentas de segurança, a praga abre um serviço na porta 36794, que é capaz de receber comandos externos, permitindo que um hacker tenha controle e acesso a todos os dados do computador infectado. O vírus permite até a ativação de um servidor Web, que liberaria o acesso aos arquivos da máquina infectada a partir de qualquer browser, o que é uma séria ameaça a segurança de qualquer rede

Como remover

A remoção do BugBear não é simples, pois envolve a alteração de chaves de registro e a exclusão dos arquivos do BugBear, que podem estar com os mais variados nomes, escondidos nas pastas de sistema do Windows. Portanto, para que a remoção seja feita com segurança, o recomendado é utilizar um antivírus atualizado, ou então as ferramentas de remoção que os próprios fabricantes de antivírus costumam oferecer em seus sites. **PCM**

Fonte: Network Associates - www.nai.com
Symantec - www.symantec.com

O custo da infecção

Toda infecção por vírus tem o seu custo. Manter os sistemas de antivírus é, por si só, um custo associado às infecções além, é claro, do custo dos dados perdidos do técnico responsável pela remoção e até do tempo perdido, por exemplo. Mas quando o BugBear infecta uma rede local, surge ainda um outro prejuízo, que se não é alto o suficiente para causar pânico, ainda assim pode provocar um grande transtorno papel

Explica-se: ao se espalhar pela rede local, o BugBear, aparentemente por um erro do programador, procura enviar-se para qualquer conexão da rede Windows que ele encontrar, seja a conexão uma pasta compartilhada ou não. Ao encontrar uma impressora compartilhada o vírus, inocentemente, tentará infectá-la. A impressora, entretanto fará com o arquivo o que faz com qualquer outro pacote de dados que recebe pela rede o imprimirá Resultado, ao infectar uma rede local, o BugBear faz com que todas as impressoras compartilhadas comecem a imprimir páginas sem sentido. Caótico, não?

Veja como sua rede é vulnerável

Conheça as principais falhas de segurança que podem causar grandes danos e comprometer o funcionamento de sua rede e aprenda a contorná-las

Por Domingo Martin Montanaro

Atualmente a maior parte das empresas está exposta a falhas de segurança em suas redes. Essas vulnerabilidades podem não só comprometer o funcionamento do sistema como provocar sérios prejuízos para a empresa e seus clientes. Algumas medidas simples, porém, podem proteger sua rede.

A seguir você verá as principais vulnerabilidades das redes e como manter a segurança de uma empresa, qualquer que seja seu porte, onde os clientes da rede são Windows e os servidores Windows e Linux.

Privilégios no computador

Permitir que um usuário tenha privilégios máximos no computador que está operando na empresa é um sério problema. Para um funcionário exercer as funções triviais e rotineiras de uma empresa, não é necessário ter privilégio de administrador no computador que está utilizando. Isso porque, como administrador, o mesmo pode utilizar recursos poderosos do sistema operacional que podem levar ao comprometimento da rede.

Para aplicar estas diretivas de acessos aos computadores na sua rede, é necessário que você tenha nas máquinas um sistema operacional multiusuário que possibilite estas definições de níveis de acesso. É importante ressaltar que um usuário comum que não tenha privilégios de administrador não tem acesso aos arquivos fundamentais do sistema operacional, assim como não tem acesso

a recursos de programação como APIs (Application Programming Interface) ou recursos da pilha TCP/IP como criar *Raw Sockets* (veja o diagrama na página 39).

Usuário comum

Existe uma imagem de disco de boot do Windows 2000 que possibilita que, no processo de incialização da máquina, o computador entre em uma mini-distribuição Linux. Esta mini-distribuição tem duas funções: editor de registro e alteração de senhas dos usuários do Windows inclusive do Administrador.

Ou seja, simplesmente com um disquete, o usuário do computador pode alterar a senha de administrador pelo Linux e logar no Windows como Administrador (inclusive se o sistema de arquivos for NTFS, uma vez que esta "mini-distribuição" possui suporte para alteração em sistemas de arquivos NTFS).

Para prevenir-se deste tipo de ataque, mantenha uma boa senha na BIOS das máquinas e deixe configurado por padrão o primeiro *Boot Device*, o HD que contém o sistema operacional à ser utilizado (normalmente IDE0).

SO monousuário

Assumindo-se que o sistema operacional dos seus clientes não seja multiusuário, existem configurações que ajudam no quesito segurança. A maioria dessas configurações constam em alterar o registro do Windows. Como esta é uma tarefa muitas vezes trabalhosa e complicada, existe um software chamado *POLEDIT*, encontrado no CD-ROM do Windows 98. Nele é possível definir muitas configurações do usuário, principalmente os recursos que o mesmo irá ter acesso ou não. O programa tem interface gráfica e é de fácil manuseio.

A auditoria de uma rede tem que ser centralizada, ou seja, tudo o que acontece na rede tem que ser fiscalizado por um servidor. Isso implica em configurações nos computadores que obrigam operações a passarem pelo servidor. Um bom exemplo disso é exigir que os usuários da rede digitem seus nomes de usuários e senhas para poder entrar no sistema operacional. Sem essa opção, simplesmente pressionando *ESC*, o usuário tem acesso ao computador.

Antigamente, a troca de informações numa rede Windows era através do protocolo NETBEUI. Hoje em dia, a maioria do tráfego é todo TCP/IP. O NetBEUI foi encapsulado dentro do TCP/IP, utilizando serviços como SMB – Server Message Block –, conhecido também como CIFS – Common Internet File System.

Poucas mas redes ainda trabalham com IPX/SPX, uma vez que há poucas redes baseadas em Novell, sistema que utiliza este último protocolo citado (e mesmo assim Novell já é compatível com TCP/IP). Quando um usuário não loga no domínio, ele tem acesso ao TCP/IP e assume um IP na rede.

Isto implica que mesmo sem autenticação no servidor, o mesmo consegue comunicação à todos os dispositivos da rede, podendo assim comprometer a segurança da rede utilizando vulnerabilidades conhecidas.

O fato de um usuário não se autenticar no domínio não o deixa incomunicável. Para forçar um usuário a logar-se no domínio para poder entrar no sistema operacional (Windows 9x), é necessário alterar a chave de registro presente em *HKEY_LOCAL_MACHINE \Network\Logon*, com o conteúdo:

Nome: MustBeValidated
Valor DWORD (hexa): 1 - irá ficar 00000001

Outra configuração interessante, é restringir o usuário a logar no domínio somente de seu computador. Isso facilita a auditoria no caso de qualquer incidente. Basta configurar em seu servidor de rede.

Sniffing

Um dos maiores e mais destruidores tipos de captura de informações numa rede é o Sniffing. Este método oferece dois grandes problemas. O primeiro é que são de difícil detecção. O outro é que são necessários muitos recursos: basta logar num computador com permissões de administrador e ter um cabo de rede plugado no PC.

O tipo de sniffing que pode ser feito em sua rede varia de acordo com o seu aparelho de comunicação (HUB ou SWITCH).

HUB: Sniffing Passivo

Um *hub* funciona da seguinte maneira: quando um pacote é enviado de uma estaçao X para uma estação Y, o HUB repete o sinal daquele pacote para todas as máquinas. De acordo com a identificação do destino, a placa de rede da estação Y irá processar o pacote e enviá-lo ao sistema operacional. Só que quando a placa de rede da máquina Y aceita este pacote, todas as outras placas de rede descartaram o mesmo, pois aquele pacote não era destinado à elas.

Existe um modo que possibilita à placa receber todos esses pacotes e diretamente enviá-los ao sistema operacional, o *Modo Promíscuo*. A partir desse ponto, é só exibi-los através de algum software. Um software grátis que faz isso muito bem é o Ethereal. Para utilizá-lo é necessário instalar o driver de captura de pacotes, ou seja, um conjunto de bibliotecas para trabalhar com o *Modo Promíscuo* da placa.

Para que se tenha uma idéia do quão destrutível este tipo de ataque é, é possível ler todos os e-mails de uma empresa inteira, utilizando apenas um simples software que trabalha com um filtro. Todos os pacotes relacionados à e mails são capturados e exibidos.

Protegendo-se de Sniffers

É importante ressaltar que uma das maneiras utilizadas para tirar proveito em uma rede invadida é rodando um sniffer na máquina onde se tem acesso. Isso faz com que um simples acesso à qualquer máquina na rede, por menos importância que ela tenha, seja um alvo em potencial para coletar senhas e dados de toda a rede.

Sniffing Passivo

Localmente: Detectar se a placa de rede está em modo promíscuo localmente é simples. Basta rodar algum programa que detecte em qual modo suas interfaces de rede encontram-se. No site da PCMaster (www.europanet.com.br/pcmaster/edicao66) você encontra o *Promiscdetect* que faz isso.

Para detectar se você está rodando um sniffer localmente, execute o */sbin/ifconfig*, e verifique a última linha da saida do comando. Se estiver escrito *RUNNING PROMISC*, é porque a placa está em modo promíscuo.

Remotamente: Existe um programa chamado *L0pht AntiSniff* que trabalha enviando pacotes para todos os endereços da rede e fazendo uma "temporização" do tempo de resposta. De acordo com esses cálculos, é possível detectar um sniffer na rede. Esta ferramenta é paga e pode ser adquirida em www.atstake.com.

Existe também uma ferramenta Open Source chamada *NEPED* que detecta sniffers especificamente na plataforma Linux remotamente, uma vez que esta plataforma é a mais utilizada para rodar os sniffers.

Sniffing Ativo

Detectar Sniffers ativos é mais simples. O próprio *ettercap* citado no texto da matéria possui essa função. Para isso, é só detectar qual máquina na rede possui entradas duplicadas na tabela ARP.

Uma boa dica para não ter que rodar um sniffer para detectar outro, é utilizar o ArpWatch. Esta ferramenta Open Source tem como fundamento notificar o Administrador da rede por mudanças na tabela ARP das máquinas. Uma vez instalado em uma máquina Linux, ele irá construir um banco de dados de endereços de rede e quando o mesmo detectar mudanças estranhas relacionadas ao ARP, enviará um e-mail ou registrará uma entrada no log do sistema. O ArpWatch está disponível também no site da revista.

Além disso, as senhas de autenticação em servidores de e-mail (POP, SMTP) normalmente trafegam como texto plano, ou seja, sem criptografia nenhuma. Todo tipo de senha digitada e que trafegará pela rede pode ser capturada.

Switch: Sniffing Ativo

Uma das maneiras mais utilizadas para o Sniffing Ativo é o ataque conhecido como "man-in-the-middle". Consiste em colocar a máquina de uma rede no meio da conexão entre outras maquinas, fazendo assim uma máquina passar-se por outra.

Um programa que funciona tanto em Linux como em Windows e que efetua este tipo de ataque chama-se "Ettercap". Este software tem a capacidade de posicionar-se no meio de duas ou mais conexões, exibindo todos os pacotes que são "trocados". Para as duas ou mais máquinas atacadas, o ataque é inperceptível. Ele funciona da seguinte maneira:

Para iniciar uma conexão IP, são necessários dois dados:

- Endereço lógico da placa de rede (Endereço IP)
- Endereço físico da placa de rede (MAC Address).

Quando é solicitada uma conexão IP, a primeira coisa que o sistema operacional faz é solicitar o endereço físico da placa de rede. Isso é feito pelo protocolo ARP, que efetua uma pergunta na rede: "Quem está utilizando o endereço IP X.Y.W.Z?". A resposta para esta pergunta contém o

endereço MAC da placa de rede, e, a partir desse ponto, é possível iniciar a troca de dados pelo protocolo IP.

O que o sniffer faz é simplesmente interceptar esse tipo de solicitação e antecipar-se à resposta, seguindo estes passos:

1 Máquina A envia solicitação de endereço MAC em *broadcast* ao IP 192.168.0.2

2 Máquina B (rodando Sniffer) responde que ela detém aquele endereço MAC, que na verdade é da máquina C.

3 Máquina B envia para máquina C pedido de conexão passando-se por máquina A.

4 Máquina C envia dados à máquina B, pensando que está comunicando-se com a máquina A, assim como a máquina A envia dados à máquina B, pensando que está comunicando se com a máquina C.

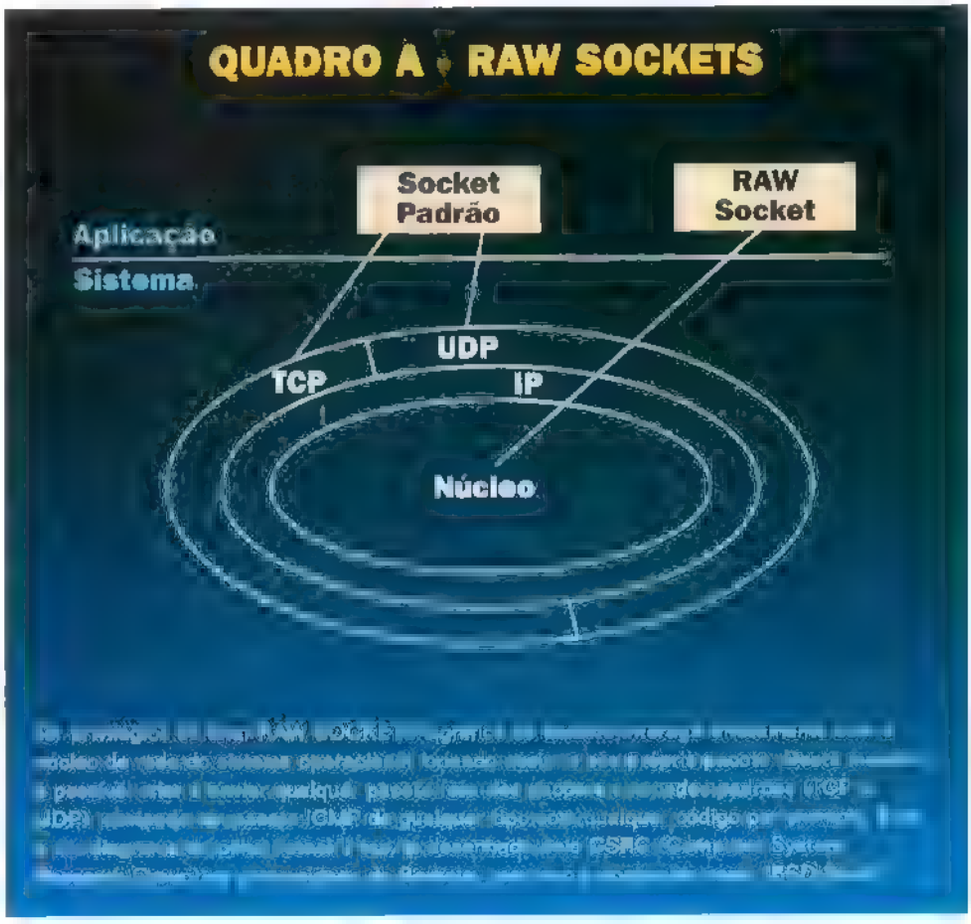
Outras vulnerabilidades

Um ataque muito praticado e que dificilmente encontra empresas protegidas, é o ataque ao compartilhamento de arquivos. Existem duas maneiras de efetuar.

1 Utilizando uma vulnerabilidade conhecida no Windows 98, da qual é possível descobrir em poucos segundos a senha utilizada em determinado compartilhamento, pois ele possui uma falha na verificação da senha.

2 Utilizando um programa de quebra de senha, o qual irá verificar, uma a uma, todas as senhas possíveis para acessar determinado compartilhamento.

Para explorar a vulnerabilidade do item 1, existem diversos programas. Um deles, muito funcional é o LanGuard Network Scanner, disponível em www.languard.com.



Para proteger-se desta vulnerabilidade é necessário executar o Windows Update e instalar as atualizações de segurança.

Já a segunda maneira de conseguir acesso a outra máquina através da rede pelo compartilhamento de arquivos é utilizando programas de quebra de senha, que utilizam força bruta para "adivinhar" senhas.

Um desses programas chama-se BRUTUS e pode ser encontrado em http://www.hoobie.net/brutus/.

Mesmo a combinação de senhas a ser tentada sendo muito numerosa e demorada, numa rede local isso é quase desapercebido. Por isso, é aconselhável que os usuários guardem seus arquivos de trabalho num servidor de arquivos.

A diferença da tentativa de um ataque em uma estação de trabalho e a tentativa de ataque em um servidor, é que o servidor possui mecanismos que bloqueiam as tentativas após um número configurado previamente. Sua política de auditoria também é muito melhor pois um servidor irá gerar logs e alertar o administrador da rede. **PCM**

Orientação a objetos e novas tecnologias de acesso a banco de dados
nas algumas das novidades do VB .NET.
ata e veja porque esta pode ser a ferramenta ideal para a sua empresa

Visual Basic de gente grande

Orientação a objetos e novas tecnologias de acesso a banco de dados são algumas das novidades do VB .NET. Veja porque esta pode ser a ferramenta ideal para a sua empresa

Por Toni Cavalheiro

Alguns a consideravam a linguagem perfeita – fácil de usar, com um bom ambiente gráfico e com um sistema de ajuda de fazer inveja ao melhor guia de consulta. Já outros só a criticavam, alegando que não havia orientação a objetos, que o acesso às bases de dados era precário e que era praticamente impossível criar aplicações *multithreading* nesta linguagem. É claro que estamos falando do Visual Basic 6, mas agora, com o novo Visual Basic .NET, as coisas mudaram para valer. Todas estas súplicas dos programadores foram atendidas e, o que é melhor, da maneira mais visual possível.

O Visual Basic .NET, pela primeira vez, aparece como um ambiente de programação extremamente poderoso e pronto para trabalhar com a Web. É o que podemos chamar de "uma linguagem para gente grande", já que muitas empresas certamente irão adotar este novo VB como sua plataforma definitiva de desenvolvimento. As mudanças foram tantas que a própria Microsoft está considerando o VB .NET a principal ferramenta do pacote Visual Studio.

No quesito portabilidade, as principais alterações estão relacionadas ao ASP.NET. Agora você pode facilmente exibir todo o conteúdo da sua aplicação em uma página Web e torná-lo acessível a sua equipe de vendas em qualquer lugar do mundo, por exemplo.

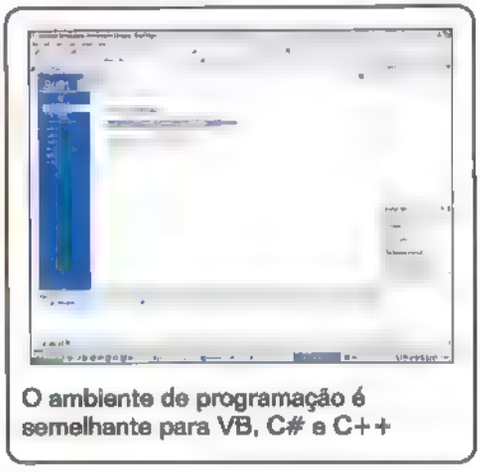
Mas talvez um dos recursos mais interessantes do .NET seja o novo sistema de acesso a bancos de dados, o ADO.NET. Não que houvesse algo de errado com os sistemas anteriores (o ODBC e o OLEDB), mas a Microsoft viu a necessidade de algo que interagisse melhor com o .NET Framework. O resultado foi excelente, criando uma tecnologia rápida, confiável e, graças ao Visual Studio .NET, fácil de usar.

A seguir você verá como funciona a nova interface do Visual Basic .NET e irá acessar uma base de dados SQL. Neste último exemplo, serão usadas apenas duas linhas de código: todo o restante será feito graficamente, através da IDE do Visual Basic .NET.

Iniciando no VB .NET

Para criar um programa que, embora seja bem simples, mostrará bem a nova interface do Visual Basic .NET, a idéia é elaborar um programa que leia três valores inteiros digitados pelo usuário e, após um clique sobre o botão Calcular, exiba o resultado no mesmo formulário. Para fazer isso, siga estes passos:

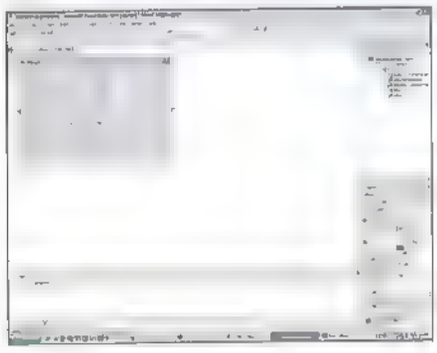
1 Execute o Visual Studio .NET, clicando em *Iniciar*, *Programas*, *Visual Studio .NET* e, novamente, em *Visual Studio .NET*. A tela principal do Visual Studio .NET será exibida. Esta tela é comum para todas as ferramentas do pacote, ou seja, o Visual Basic, o C# e o C++. Clique em *New Project* para iniciar um novo projeto e, na tela que aparecer, selecione *Visual Basic Projects* e dê um clique duplo sobre *Windows Application*.



O ambiente de programação é semelhante para VB, C# e C++

2 A tela principal do *Visual Basic .NET* será iniciada e o formulário aparecerá na janela central. Repare que do lado esquerdo há um menu chamado

Toolbox. É nele que estão todos os objetos que você usará no desenvolvimento deste programa. Passe o mouse sobre ele para expandi-lo e arraste os seguintes controles para o formulário: quatro *Labels*, três *TextBox* e um *Button*. A figura abaixo mostra como eles devem ser posicionados.



Arraste para o formulário os controles necessários para o aplicativo

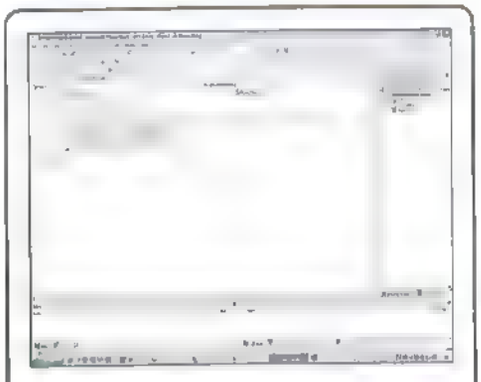
3 Agora chegou a hora de personalizar a interface do seu programa. Clique sobre cada uma das *Labels* que você inseriu (uma por vez) e repare que as propriedades correspondentes a elas aparecerão no menu *Properties*, no canto inferior direito da tela. Localize a propriedade *Text*, que está disponível no submenu *Appearance*, e adicione os seguintes nomes para cada uma das *Labels*: *Valor 1*, *Valor 2*, *Valor 3*. Deixe a propriedade *Text* da última *Label* em branco.

A interface da aplicação terá uma estrutura como a indicada acima

4 Clique sobre o botão e altere sua propriedade *Text* para *Somar*. Além disso, clique sobre cada um dos *TextBox* e deixe os controles *Text* correspondentes a eles em branco. Após fazer todas estas alterações, a interface do seu programa deverá estar como a da figura anterior.

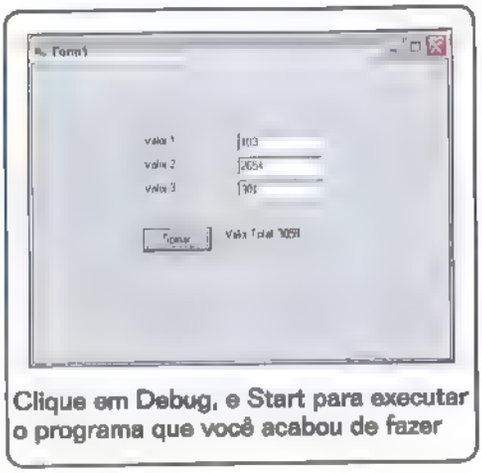
5 Finalmente você está prestes a entrar na parte divertida da programação: os códigos. Dê um clique duplo sobre o botão para acessar a janela de códigos do Visual Basic .NET. Agora digite o seguinte programa entre as linhas *Private Sub* e *End Sub*.

```
Dim valor1 As Integer =
CInt(TextBox1.Text)
Dim valor2 As Integer =
CInt(TextBox2.Text)
Dim valor3 As Integer =
CInt(TextBox3.Text)
Dim total As Integer = valor1 +
valor2 + valor3
Label4.Text = "Valor Total: " & total
```



Com um duplo clique sobre o botão você tem acesso a janela de códigos

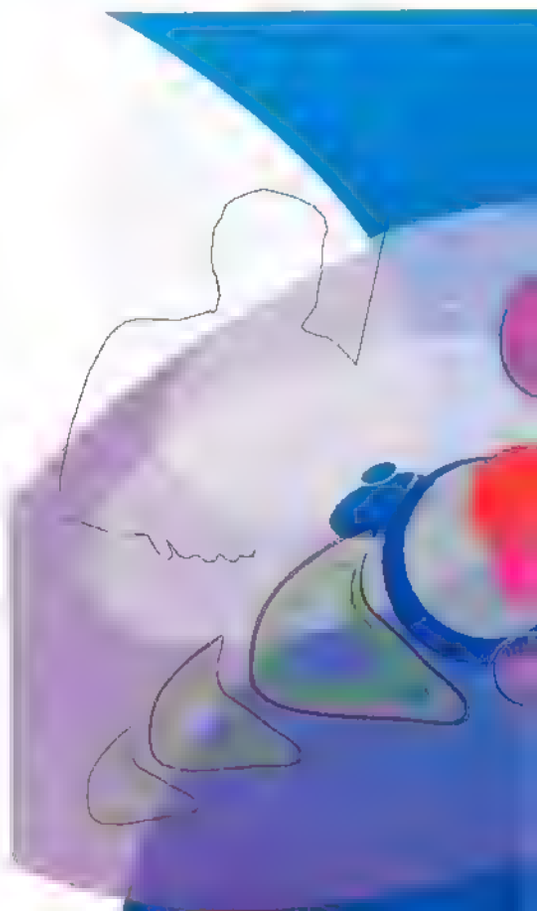
6 Rode o programa clicando em *Debug* e selecionando *Start*. O código será compilado e, caso não ocorra nenhum erro, uma janela com o seu aplicativo aparecerá na tela.



Clique em Debug, e Start para executar o programa que você acabou de fazer

Teste-o para ver se tudo está funcionando corretamente.

Pronto, você acaba de criar sua primeira aplicação no Visual Basic .NET. Porém, este programa ainda não está pronto para ser distribuído. Dê uma olhada na barra de ferramentas do Visual Basic .NET e repare que há uma caixa com a palavra *Debug*. Isto significa que a aplicação foi compilada apenas para teste. Antes de compilar a versão final, lembre-se de mudar esta caixa para *Release*. Depois, é só acessar a pasta do seu programa.



geralmente localizada em *Meus Documentos*, *Visual Studio Projects*, e copiar o arquivo executável que está dentro da pasta *Bin* do seu projeto.

SQL em duas linhas

A moda não vem de hoje: sempre que uma nova versão é lançada, o Visual Basic vai ficando mais visual. Prova disto são os novos métodos de acesso a bases de dados SQL através do ADO.NET, uma tecnologia essencial para qualquer empresa da atualidade, independente do porte ou da quantidade de funcionários.

Para ilustrar como estas novidades funcionam, veja um exemplo que lê uma tabela da base de dados, exibe o conteúdo na tela e, através de um botão chamado *Update*, permite que o usuário final altere os dados. Tudo isso com apenas duas linhas de código. Todo o restante do acesso à base de dados será feito através de ferramentas visuais.

1 Antes de qualquer coisa, você deve ter o SQL Server 7.0 ou 2000 instalado em uma das máquinas da rede. Caso você não tenha, entre no endereço www.microsoft.com/sql, baixe uma versão de avaliação para 120 dias e instale o produto.

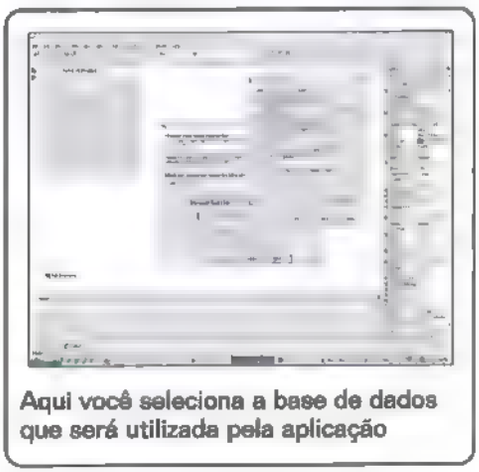
2 Durante a configuração do SQL Server, você deve ficar atento a alguns pré-requisitos. Primeiramente, selecione o modo de autenticação baseada em Windows e, na próxima tela, opte pela autenticação mista. Deixe o usuário *sa* sem senha, embora isto não seja recomendável em uma situação real. Após a instalação, não se esqueça de ativar o SQL usando o Service Manager. Neste exemplo, usaremos a tabela *Authors* da base de dados *Pubs*, que já vem configurada como padrão no SQL Server.

3 Execute o Visual Studio .NET e inicie um novo projeto Windows Application do Visual Basic .NET. Após fazer isto, o novo projeto será carregado e um formulário será exibido na tela.

4 Usando a *Toolbox* do lado esquerdo da tela, clique na guia *Data* e arraste um objeto *SqlDataAdapter* para o formulário. Um assistente de configuração aparecerá, sendo que a primeira tela é somente informativa. Portanto, clique em *Next*.

5 Agora você deve selecionar a conexão de dados. Dependendo de suas tentativas anteriores, é possível que já apareça alguma conexão predefinida. No entanto, clique em *New Connection* para criar uma conexão do zero.

6 Esta tela é uma das mais importantes. É nela que você irá selecionar a base de dados que será utilizada. Selecione o servidor SQL, digite *sa* no campo *user name* e marque a opção *blank password*. Escolha também a base de dados pubs e clique no botão *Test Connection* para confirmar se tudo está funcionando. Em seguida, clique em *OK*.



Aqui você seleciona a base de dados que será utilizada pela aplicação

7 O programa voltará para a mesma tela do passo 5. Selecione a conexão que você acaba de criar e, em seguida, clique em *Next*. Na próxima tela que aparecer, deixe a primeira opção selecionada (Use SQL statements) e clique em *Next* novamente. Uma nova tela aparecerá pedindo que você entre com uma query SQL. Digite o comando abaixo e clique em *Finish*.

```
Select * from Authors
```

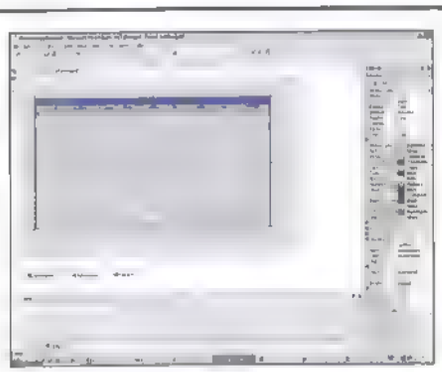
Após selecionar a base de dados, selecione o item Use SQL statement

8 Devolta ao formulário principal repare que apareceu uma nova opção no menu de comandos: a opção *Data*. Clique sobre ela e escolha *Generate Dataset*. Na nova

tela que aparecerá, selecione *New*, chame este novo *DataSet* de *dsAuthors* e clique em *OK*. Neste ponto do desenvolvimento, você terá três objetos abaixo do formulário: *SqlDataAdapter1*, *SqlConnection1* e *DsAuthors1*.

9 De volta à *Toolbox*, clique na guia *Windows Forms*, arraste um controle *DataGrid* para o formulário e altere seu tamanho. Se desejar, clique com o botão direito do mouse sobre ele e escolha um dos estilos predefinidos. Minha sugestão pessoal é o *Professional2*, mas você pode optar por qualquer estilo.

10 Agora chegou a hora de ligar o *DataGrid* ao *DataSet*. Clique no *DataGrid* e, na janela *Properties*, localize a propriedade *DataSource*. Configure-a para *DsAuthors1*. Mude também a propriedade *DataMember* para *Authors*. Sua tela deve estar parecida com a da figura a seguir.



Altere as propriedades do DataGrid, DataSource e DataMember

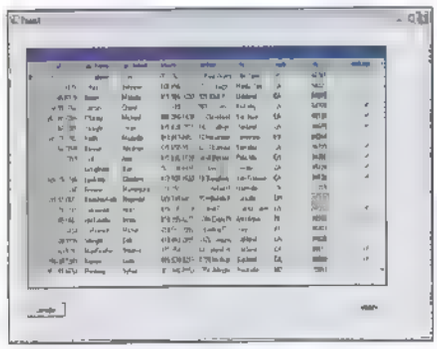
11 Para finalizar, arraste dois controles *Button* para o formulário e posicione-os um pouco abaixo do *DataGrid*. Chame o primeiro de escrever *Carregar* (alterando a propriedade *Text* do botão) e o segundo de *Update*. Mude também a propriedade *Name* dos dois botões para *cmdLoadData* e *cmdUpdateData*, respectivamente.

12 Agora só resta adicionar o código dos botões. Para fazer isto, dê um clique duplo no botão *Carregar* e entre com a seguinte linha de código para o procedimento:

```
SqlDataAdapter1.Fill(DsAuthors1)
```

Dê também um clique duplo no botão Update e entre com o seguinte código para o procedimento:

```
SqlDataAdapter1.Update(DsAuthors1)
```



Ao executar o programa será exibido o conteúdo da tabela SQL

Pronto, seu programa está terminado. Para conferir se tudo está funcionando corretamente, compile e execute a aplicação clicando em *Debug*, *Start* ou pressionando a tecla F5. Você verá uma tela parecida com a da figura acima.

Para testar a aplicação, pressione o botão *Carregar* e confira se os dados aparecem na tela. Depois, altere ou adicione um item qualquer na tabela e aperte *Update* para enviar os dados. Você acaba de criar uma tabela totalmente funcional usando apenas duas linhas de comando.

Este é apenas um dos exemplos que mostra a facilidade que o novo Visual Basic .NET proporciona. Daqui para frente é com você. Consulte sempre a documentação online do Visual Studio .NET e em pouco tempo é possível desenvolver ótimas aplicações comerciais digitando o mínimo de código possível. Afinal, o Visual Basic nunca esteve tão visual quando esta versão .NET **PCM**

Fale conosco: www.conectiva.com.br
decli@conectiva.com.br
Filiais: (41) 360 2640 Curitiba/(11) 3266 5888 São Paulo
(21) 2515 4888 Rio de Janeiro/(61) 322 4800 Brasília/(51) 3211 0036 Porto Alegre

Mandrak Linux 9

Conheça a mais nova versão do Mandrake Linux, que você recebe nos CDs-ROM desta edição

O Mandrake vem se destacando entre os usuários pela sua simplicidade e facilidade de uso, principalmente na instalação e na configuração. A nova versão deste Linux é o Mandrake 9, que você recebe nos dois CDs-ROM desta edição da PC Master.

Entre os motivos do sucesso desta distribuição, além de sua descomplicação, pode-se destacar o tratamento recebido pelo sistema para que se torne cada vez mais amigável. Um bom exemplo pode ser observado no gerenciador de janelas padrão, o KDE (versão 3.0.3). Ele está muito semelhante ao ambiente do Windows, o que facilita a adaptação de novos usuários neste sistema operacional.

Ao se instalar esta distribuição em seu computador, são colocados também centenas de aplicativos com as mais diversas finalidades. Pode-se encontrar jogos, ferramentas para Internet e até aplicativos para se montar os mais diversos servidores.

São muitas as novidades que foram incluídas nesta nova versão do Mandrake Linux. Entre elas, destaca-se o Mandrake Control Center, uma ferramenta que permite a configuração em seus dispositivos e também no sistema, tudo através de uma interface gráfica. Através dele, é possível configurar o firewall e também compartilhar o seu acesso a Internet sem a necessidade de comandos complexos.

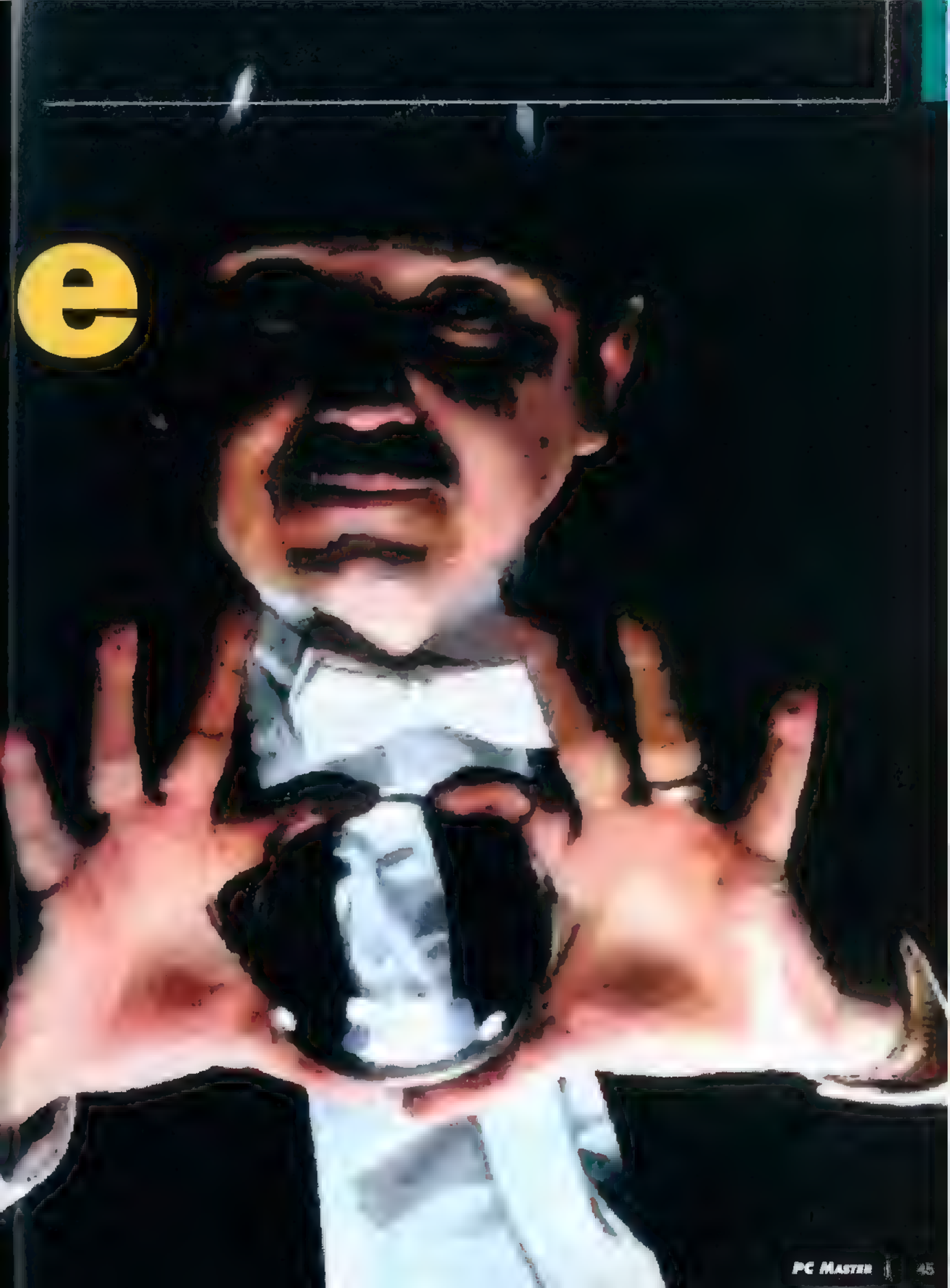
Outra novidade nesta nova versão do Mandrake é o pacote de ferramentas OpenOffice, que foi incluído no sistema após o lançamento da versão estável deste software. O pacote é formado por editor de texto, planilha de cálculo, software de apresentação entre outras aplicações.

Além do pacote OpenOffice também estão incluídas outras ferramentas, entre elas o KOffice, aplicativos de servidor como o Apache e navegadores Internet como o Mozilla, o Konqueror e o Nautilus. Estes dois últimos são ferramentas do KDE e Gnome respectivamente. Como curiosidade, ambas as ferramentas são semelhantes ao Explorer do Windows que pode ser usado como gerenciador de arquivos e também como Browser.

Veja agora o passo-a-passo de como fazer a instalação deste sistema operacional, em seguida conheça as principais novidades desta versão do Mandrake que tornam esta distribuição Linux uma das principais existentes.

Antes de instalar

Assim como qualquer sistema operacional, o Mandrake Linux pode causar perda de dados no seu disco rígido no momento da instalação. Por este motivo é altamente recomendável que você faça um backup de todas as informações importantes antes de iniciar qualquer procedimento descrito nesta reportagem.



Instalação

Iniciar a instalação do Mandrake 9 em seu computador é muito fácil, basta acompanhar os passos a seguir para esclarecer suas dúvidas.

1 Coloque o CD-ROM em sua unidade de CD e inicie o computador. A tela de instalação deverá aparecer. Pressione *Enter* para prosseguir. O instalador será carregado e irá solicitar a língua em que deverá ser realizada a instalação. Selecione Português, Brasil.

2 Será exibido o termo de licença, pressione *Aceitar* para continuar a instalação. Você deve informar agora se deseja realizar uma instalação ou uma atualização. Se estiver instalando Linux pela primeira vez, escolha as opções *Recomendado* e *Instalar* para que o processo seja o mais simples.

3 Será exibida uma lista com diversos modelos de teclados, selecione o correspondente ao seu e pressione *Ok*.

4 O sistema perguntará se deseja utilizar o espaço em disco livre ou particionar o disco manualmente. É necessário que você tenha uma partição livre para realizar a instalação do sistema. Crie pelo menos uma partição Linux Nativa com ponto de montagem / e uma partição de swap. Para ter mais detalhes, leia o quadro *Particionamento de disco*, na página ao lado.

5 Será exibida uma lista de pacotes que podem ser instalados em seu computador. Selecione os que deseja e pressione *Ok* para confirmar. Os pacotes serão copiados para o disco.

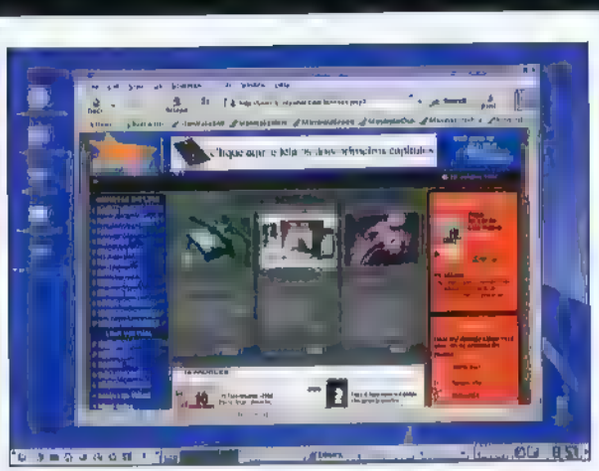
6 Durante a instalação, o sistema irá solicitar que o CD seja substituído. Neste momento, retire o CD 1 da sua unidade e coloque o segundo disco, pressionando *Enter*. Em algumas instalações é pedido um terceiro CD, se for o seu caso, pressione *Cancelar*.

7 Com todos os arquivos copiados em seu computador, o sistema irá realizar as configurações finais do sistema. Será solicitado que você informe a senha do root. Este é o usuário administrador do sistema, digite a senha para ele.

8 Em seguida, você pode criar usuários que utilizarão o sistema. É recomendada a utilização normal através de uma conta de usuário sem privilégios de administrador. Isto evita que ocorram acidentes no sistema.

9 Se possuir um dispositivo de rede, o sistema normalmente detecta automaticamente. Marque o tipo de rede na qual seu computador está conectado.

10 Informe ao sistema os dados de sua rede local, como endereço IP, máscara e servidor de nome. Caso não saiba estas informações, consulte o administrador de rede.



O ambiente gráfico padrão do Mandrake é o KDE, que é muito semelhante ao Windows

Disco de boot

Se o seu computador não pode dar boot pelo CD ROM e os outros métodos não funcionaram, você deve criar um disco de boot no Windows da seguinte maneira:

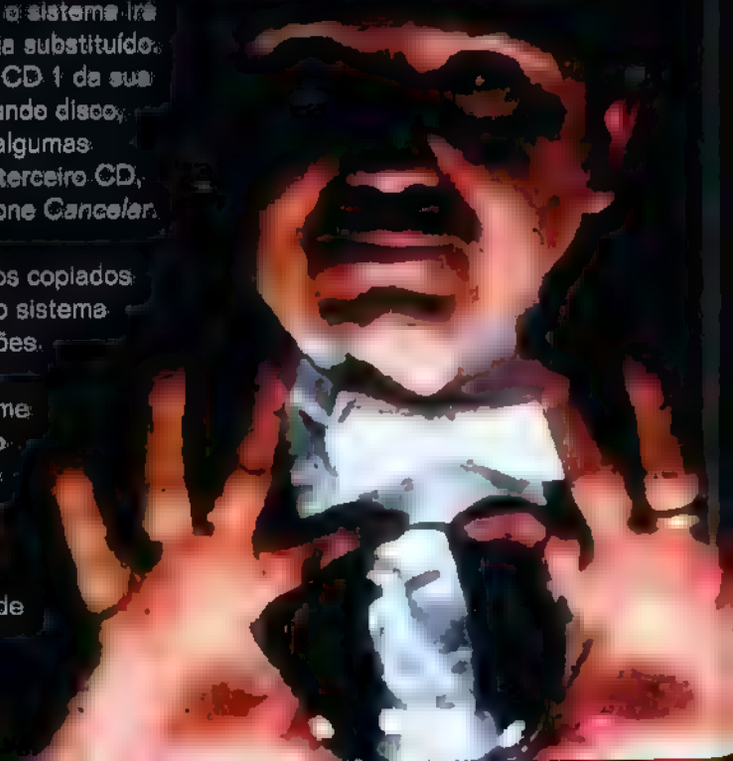
1 Insira o CD-ROM, então abra o *Meu Computador*, clique o botão direito no ícone do drive de CD-ROM e escolha *Abrir*.

2 Vá no diretório *dosutils* e clique duas vezes no ícone *rawwritewin*. Insira um disquete vazio no drive.

3 Selecione *D:\images\cdrom.img* no campo *Image File* (assumindo que seu drive de CD-ROM é *D:*, caso contrário, substitua o *D:* pela unidade de seu drive).

4 Selecione *A:* no campo *Floppy Drive* e então clique em *Write*.

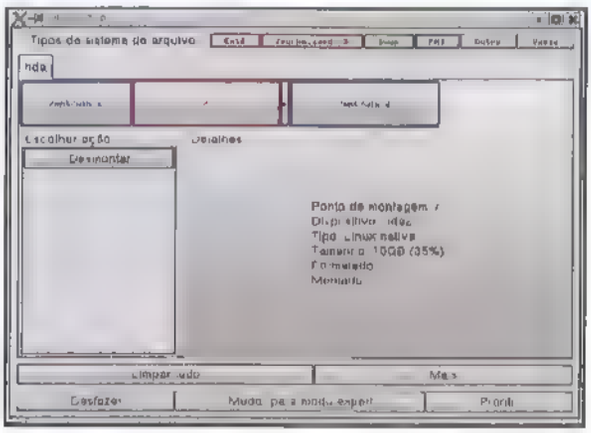
Para começar a instalação, insira o CD ROM no drive, como também o disquete de boot se necessário, e então reinicie o computador.



Particionamento de disco

O Diskdrake é a ferramenta desenvolvida especialmente pela Mandrake que permite administrar e redimensionar o tamanho das partições existentes no seu sistema. Esta ferramenta é acessada durante a instalação quando se escolhida a opção de *particionamento personalizado*.

Mas antes de realizar esta tarefa é altamente recomendável que se realize um backup do conteúdo do seu HD, pois o redimensionamento do disco pode provocar erros no conteúdo. Outra dica para evitar problemas é desfragmentar o disco.



O Diskdrake é uma ferramenta que permite particionar e redimensionar as partições de disco

A interface é dividida em quatro partes. Na parte superior, é mostrada a estrutura atual do disco rígido. Quando realizada alguma modificação nas partições, a alteração na estrutura do disco é exibida em tempo real.

Já na parte esquerda, é exibido um menu relacionado à partição selecionada na estrutura do disco rígido. Na janela da direita é apresentada a informação relativa a partição. E na parte inferior, são exibidos botões relacionados a ações gerais do disco, como limpar todas as partições, desfazer as alterações realizadas e gravar todas as alterações.

O processo para particionar um disco rígido segue um padrão. A situação mais comum é um disco com Windows instalado mas com espaço suficiente para o Linux. Nesse caso, o procedimento adotado deve ser iniciado com a verificação do espaço disponível em seu disco rígido e com a determinação do espaço para o Linux.

Antes de realizar qualquer operação, desfragmente o disco no próprio Windows e faça a cópia de segurança de seu disco.

Com todo o procedimento anterior realizado, inicie o processo de redimensionamento de disco. Selecione com o mouse a partição *Windows* na parte superior da janela do DiskDrake. Com este procedimento, será exibido um menu na lateral esquerda. Pressione o botão Redimensionar. Será exibida uma barra com o total da partição selecionada.

Existem duas formas de modificar o tamanho da partição. Na primeira, basta informar o tamanho da nova partição na caixa de diálogo. Na outra, é preciso arrastar a barra que representa o tamanho total da partição para a posição desejada. Após definir o novo tamanho, basta pressionar o botão aceitar para que a nova partição seja definida.

Depois de criar uma partição livre para a instalação do Linux você deve criar as partições para a instalação do sistema. Basicamente você precisa criar duas partições: uma nativa, com ponto de montagem / e uma partição de swap para uso da memória virtual. Mas se tiver dúvidas de como particionar o disco existe uma opção no DiskDrake que permite criar as partições automaticamente.

Selecione a partição livre na janela superior e pressione o botão *Auto-alocar* localizado na parte inferior da janela. O sistema irá criar o melhor particionamento baseado no espaço de disco disponível.

11 Será exibido ao final deste processo um resumo das configurações de alguns dispositivos que estão conectados.

12 O sistema irá configurar o servidor X (ou o modo gráfico do Linux). O Conectiva Linux tenta fazer a detecção automática da maior parte dos dispositivos existentes no mercado brasileiro. Portanto, é altamente recomendável que você use o adaptador detectado como padrão do sistema. Caso a sua placa de vídeo não seja detectada, clique em *Selecionar a placa de vídeo manualmente* e escolha o modelo do seu dispositivo.

13 Ao final a sua instalação do Mandrake Linux 8.0 estará completa e pronta para ser testada. Pressione o botão *OK* para que o sistema seja iniciado e entre no Linux.

Ao iniciar o computador, será exibido um menu em que você poderá selecionar o sistema que será inicializado. Com ele já carregado, será solicitado que você informe o nome do usuário e a senha usada durante a instalação. Caso não tenha cadastrado um usuário adicional, entre no sistema como root.

Pronto, você já está utilizando o sistema Mandrake Linux. Agora veja como funciona o Centro de Controle, que realiza a configuração no sistema, e alguns dos aplicativos disponíveis.

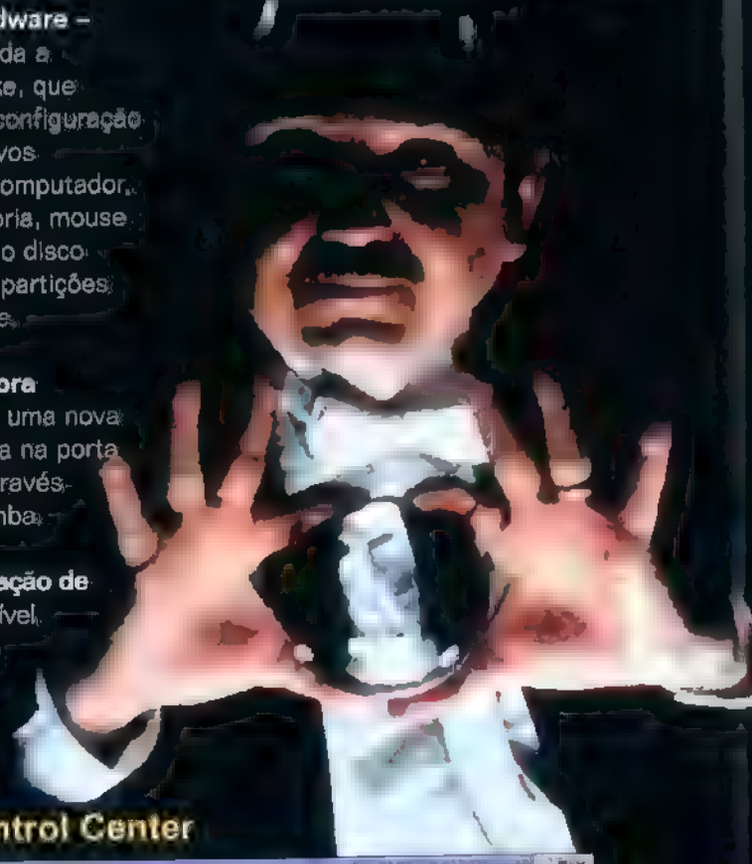
Configuração do Sistema

A configuração do sistema é feita através do Centro de Controle Mandrake, que nesta versão recebeu novas funcionalidades.

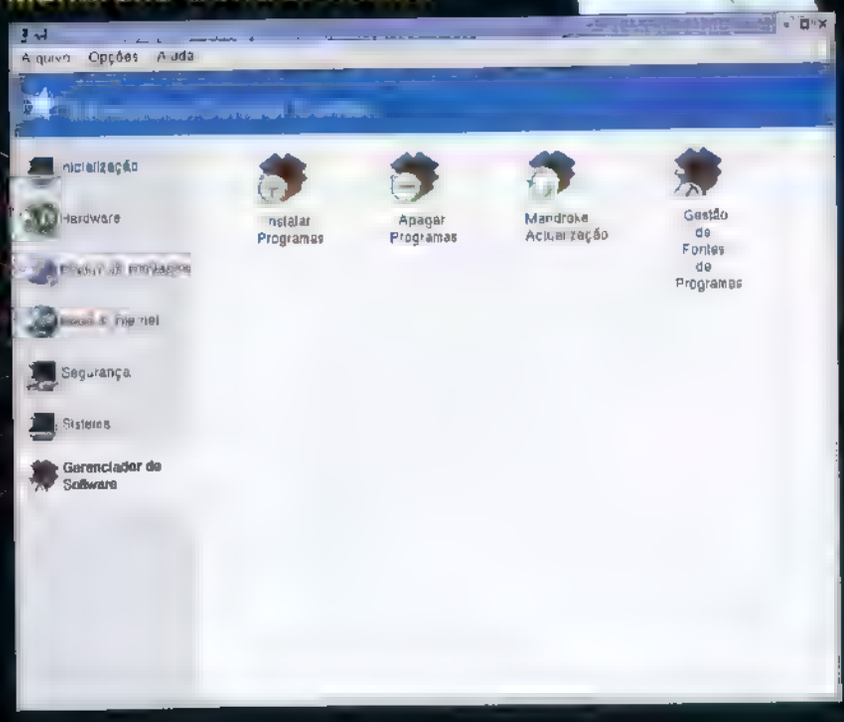
Para quem não sabe, o Centro de Controle é a principal ferramenta de configuração da distribuição Mandrake. Ele permite que o administrador do sistema faça a configuração de hardware e dos serviços do sistema. Esta ferramenta permite simplificar o trabalho de

administração do sistema com uma interface gráfica, evitando assim realizar inúmeros comandos em uma janela de terminal. A seguir, você encontra algumas das tarefas que são possíveis de se realizar com o Centro de Controle:

- **Criar um disquete de Boot** – Se durante a instalação você não criou um disquete de boot do sistema, basta colocar um disquete em sua unidade e selecionar esta opção para criar um.
- **Configuração de Boot** – Esta opção permite que você selecione a forma que o boot será realizado. É possível selecionar se o boot será feito em modo gráfico, chamado de *Aurora*, ou em modo texto. E ainda, se a tela de login deve ser realizada através de uma janela Xwindow, se o sistema deve executar o login automaticamente e se deve carregar algum dos gerenciadores gráficos disponíveis.
- **Trocar a resolução de seu monitor** – Permite alterar suas configurações de vídeo e testar se a configuração está correta. No modo *expert*, você poderá modificar a configuração do dispositivo de vídeo, do mouse, do teclado e do monitor rapidamente.
- **Configurar seu Hardware** – Nesta opção é utilizada a ferramenta *HardDrake*, que possibilita realizar a configuração de todos os dispositivos conectados em seu computador, inclusive CPU, memória, mouse, teclado, webcams, e o disco rígido, acessando as partições através do *DiskDrake*.
- **Configurar impressora** Possibilita configurar uma nova impressora conectada na porta paralela, remota e através de uma conexão Samba.
- **Trocando a configuração de seu teclado** – É possível substituir o layout do teclado que estiver sendo usado.
- **Gerenciando os pacotes** – Nas versões anteriores era carregado o aplicativo RPMDrake, que era muito mais complexo de gerenciar. No Mandrake 9, são exibidas listas de softwares disponíveis para instalar, remover e também atualizar a versão dos programas instalados no sistema.



Mandrake Control Center



Permite a configuração de dispositivos de hardware

Cria discos de boot e altera as configurações de boot

Altera as configurações relacionadas às partições de disco

Configuração de dispositivo de Rede e Internet

Configuração de firewall e outros recursos de segurança

Configuração do sistema

Gerenciador de softwares instalados

Aplicativos disponíveis

A nova versão do Mandrake Linux 9 possui muitos aplicativos que são instalados automaticamente com o sistema. Estes softwares servem às mais diversas finalidades, para quem utiliza o computador no dia-a-dia.

KDE

O gerenciador de janelas KDE (K Desktop Environment), padrão do Mandrake, é muito poderoso e fácil de utilizar. Ele possui inúmeros recursos gráficos, funcionalidades e facilidades para o usuário.

KOffice 1.2

O gerenciador de janelas KDE possui um pacote de ferramentas Office desenhado especialmente para este ambiente gráfico. Hoje o software se encontra na versão 1.2. Este pacote de ferramentas é instalado com o KDE durante a instalação do sistema.

Mas nada impede que os aplicativos funcionem em outros gerenciadores, desde que o pacote de bibliotecas esteja instalado no sistema. Assim, o usuário pode executar o Kword, que é o editor de texto no ambiente WindowMaker sem que haja qualquer problema. Este pacote é formado por um editor de texto e uma planilha de cálculo e de apresentação.

OpenOffice

O mecanismo principal deste pacote Office é o mesmo usado no StarOffice da Sun.

Pouco tempo depois de ter adquirido o StarOffice e o tornado um software gratuito, a Sun também abriu o código-fonte do mecanismo principal do software para a comunidade de desenvolvedores.

A partir deste momento, este projeto foi chamado de OpenOffice, mas sem seguir o termo de licença GPL – que obriga que os aplicativos gerados a partir de um código-fonte aberto também devem obedecer estas mesmas características.

Com o lançamento da versão estável 1.0, várias distribuições vêm adotando este software como padrão no sistema. Como não poderia ser diferente, o Mandrake Linux também é totalmente compatível com a versão 6 do StarOffice.

Licq

O Licq lembra muito o ICQ para Windows. Ele permite que você se comunique com outros usuários que utilizam este software e use até mesmo um UIN já existente.

Evolution

O Evolution é um cliente de e-mail que você encontra no Mandrake. Sua interface é muito similar à do Microsoft Outlook e os recursos não ficam para trás dos de programas comerciais. O software é composto de caixa de correio, agenda, gerenciamento de tarefas, lista de contatos e ainda informações de várias fontes de notícias. PCM

Aplicativos Disponíveis

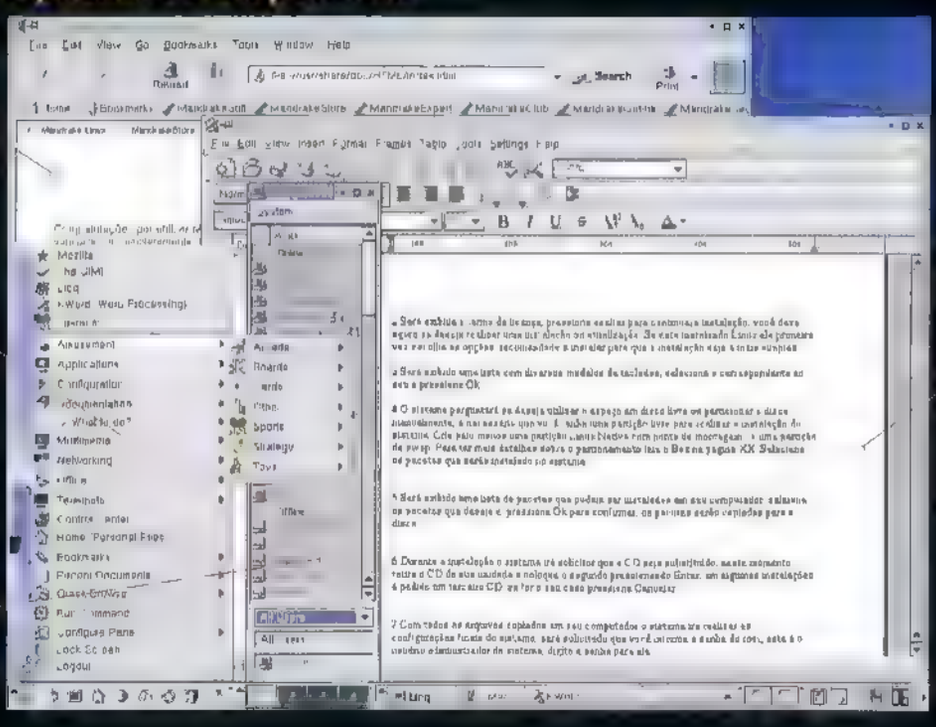


Ilustração: Rodrigo Mota

Autenticação Integrada no GNU/Linux

Aprenda como autenticar usuários de estações Linux usando o Network Information System

Por Fernando Lozano
www.lozano.eti.br
fernando@lozano.eti.br

A maioria dos sistemas GNU/Linux em uso hoje são verdadeiras ilhas de informação, pois cada um é um sistema multi-usuário autônomo, com suas próprias definições de usuários e senhas. São como servidores Netware 3.x ou estações Windows NT/2000/XP em grupo de trabalho.

Enquanto o GNU/Linux é utilizado apenas como servidor para web, firewall, e-mail ou proxy, ou quando estamos em redes pequenas onde um único servidor de arquivos rodando Samba atende a toda a rede, não há nenhum problema. Mas quando a rede passa a ter vários servidores, ou quando o GNU/Linux é utilizado também em estações de trabalho, sente-se a falta de um "login de rede", que permita acessar qualquer estação ou servidor com a mesma senha.

Muitos administradores Linux não sabem, mas qualquer distribuição têm mecanismos tão ou mais poderosos que os fornecidos pelo Netware e pelo Windows como por exemplo NIS, PAM, Kerberos e LDAP.

Autenticação x Profiles

É preciso fazer a distinção entre duas capacidades que podem ou não ser fornecidas pelos mecanismos citados

- **Autenticação:** é a capacidade de, dado um nome de usuário (login) validar a senha fornecida e assim estabelecer (ou não) uma seção com o sistema operacional.

- **Profiles:** são as definições de características do usuário para o sistema operacional, como o diretório home ou o shell padrão

Em um sistema Unix tradicional (tal qual o GNU/Linux, Solaris ou o FreeBSD), tanto a autenticação quanto os profiles são baseados nas informações contidas no arquivo */etc/passwd*. Este mecanismo foi aperfeiçoado com a separação das informações de profile e autenticação respectivamente nos arquivos */etc/shadow* e */etc/passwd*, de modo a dificultar ataques locais baseados em crackers de senhas.

Sistemas Unix tradicionais também suportam o Network Information System, ou NIS, que consiste em um conjunto de *daemons yp**. Servidores NIS utilizam bancos de dados *dbm* gerados a partir dos aquivos no diretório */etc*. Clientes NIS rodam o *ypbind*, que intercepta chamadas às funções *getpw** da LibC (ou *glibc* no Linux) e obtêm as informações à partir do NIS.

O NIS é capaz de fornecer tanto o serviço de autenticação quando os profiles dos usuários integrando servidores e estações Linux, FreeBSD, Solaris e outros sistemas Unix-like.

A necessidade de integração com mecanismos de autenticação "estrangeiros" levou à criação do PAM (Pluggable Authentication Modules), que permite autenticar senhas de uma estação GNU/Linux contra servidores Windows ou Netware. Entretanto, o PAM não fornece serviços de profile, de modo que seu uso exige que se administre usuários nos dois sistemas de forma independente, ganhando apenas a comodidade de uma senha única.

Já o Kerberos é focado em fornecer a autenticação (não profiles) em rede de forma totalmente segura, coisa que os mecanismos tradicionais do Windows e do Unix não conseguem. O risco é baixo na maioria dos ambientes de rede local ou de WAN corporativa, mas se torna significativo quando há contato com redes externas, como a Internet. Portanto, usuários de NIS devem manter seus servidores e estações do lado de dentro do firewall e não integrar os servidores públicos. No Windows 2000 com Active Directory, um porte do Kerberos cuida de toda a autenticação.

Sistemas como o OpenLDAP são a alternativa mais nova. É a mesma tecnologia utilizada como base pelo NDS da Novell e pelo Active Directory da Microsoft. O LDAP pode fornecer ambos os serviços de autenticação e profiles dos usuários, com a vantagem de ser extensível e escalável para redes com milhares de servidores e estações. Em teoria, o mesmo conjunto de servidores LDAP poderia atender aos mundos Windows, Netware e Unix de forma integrada.

Mesmo em redes puramente Unix a tecnologia LDAP ainda envolve algumas dificuldades de implementação. Uma delas é o fato de que nenhum dos front-ends administrativos a que estamos acostumados (Webmin, Linuxconf, Kusers, entre outros) é capaz de utilizar LDAP, embora eles possam ser configurados para trabalhar com o NIS.

Implementando um servidor NIS

No momento, o NIS é a tecnologia de integração de usuários mais fácil de instalar, configurar e administrar no GNU/Linux. Em primeiro lugar, você deve instalar o servidor NIS, fornecido pelo pacote

ypserv.rpm* na maioria das distribuições (ou equivalente para Debian e Slackware). Também será necessário instalar o *yp-tools*.rpm* e o *portmap*.rpm*.

Deve-se estabelecer um nome de domínio NIS (não confundir com domínios DNS ou Windows NT). O comando *nisdomainname* permite estabelecer ou retornar o nome do domínio. Neste exemplo será utilizado o domínio "pcmaster". Em seguida deve-se iniciar o *ypserv*. No Red Hat, utilize o comando:

```
service ypserv start
```

Pode-se também invocar diretamente o script de inicialização do serviço:

```
/etc/rc.d/init.d/ypserv start
```

Agora é preciso gerar os bancos de dados dbm. Isso pode ser feito pelo comando

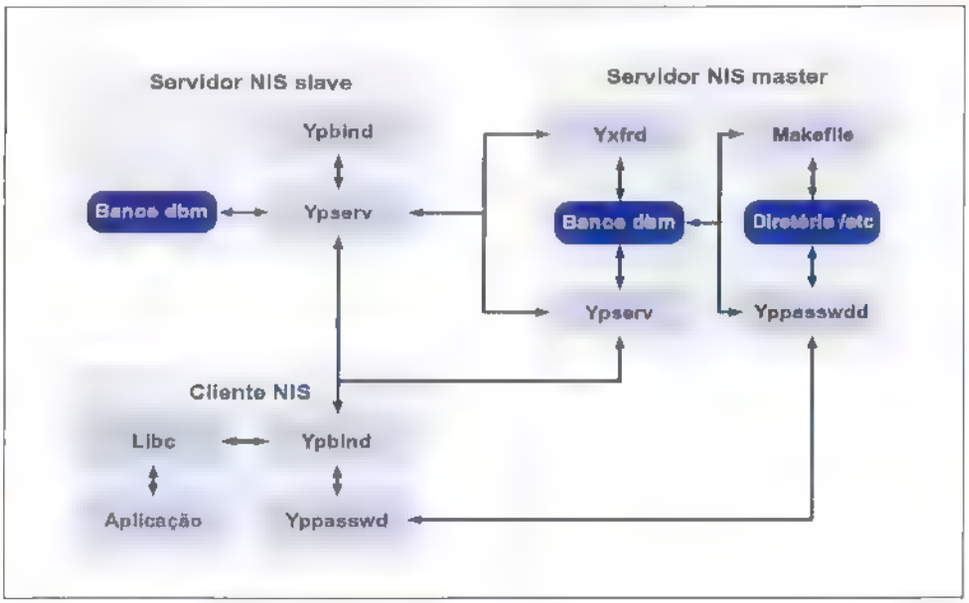
```
/usr/lib/yp/ypinit -m
```

A opção *-m* indica que este servidor está sendo configurado como *master*. Mais adiante você verá como configurar servidores *slave* para replicação da base de dados NIS.

A geração dos bancos de dados *dbm* do NIS é controlada por um Makefile armazenado em */var/yp*. Em algumas distribuições este Makefile precisa ser editado para funcionar corretamente. Procure pela linha:

```
all: passwd group hosts rpc
services netid protocols mail \
  # netgrp shadow publickey
networks ethers bootparams
printcap \
  # amd.home auto.master auto.
home auto.local passwd.adjunct \
  # timezone locale netmasks
```

Caso você observe alguma mensagem de erro na execução do *ypinit*, comente o nome do mapa que gerou o erro e em seguida reexecute o comando.



Outra modificação que pode ser necessária envolve as linhas

```
MINUID=500
MINGID=500
```

Elas estabelecem os menores UID e GID que serão incluídos nos bancos de dados do NIS. Os arquivos */etc/passwd*, */etc/shadow* e */etc/group* locais não deixam de ser utilizados em

Implementação de servidores NIS slave

Em redes pequenas, um único servidor NIS será capaz de fornecer autenticação e profiles para todos os servidores e estações. À medida que a rede cresce, no entanto, é interessante ter mais servidores NIS para dividir a carga de trabalho, para fornecer tolerância à falhas, ou gerenciar o tráfego em links de WAN.

O NIS suporta replicação master/slave, semelhante a domínios do Windows NT, de modo que todas as modificações nos bancos de dados devem ser feitas no servidor master, mas os clientes podem obter serviços de qualquer um dos servidores slave.

Em primeiro lugar, o servidor NIS master deve indicar no arquivo */var/yp/ypservers* os nomes de todos os servidores NIS do domínio (incluindo o master). Depois é preciso configurar o nome do domínio no slave, iniciar o *ypserv* e inicializar a réplica do banco de dados com o comando:

```
/usr/lib/yp/ypinit -s hostname
```

Onde hostname é o nome do servidor NIS master para o domínio.

Quando atualiza-se os bancos de dados no master, as modificações não são propagadas automaticamente para os slaves. Deve-se editar o Makefile trocando o valor "true" na linha abaixo para "false":

```
NOPUSH=true
```

Opcionalmente pode-se ativar no servidor NIS master o *daemon ypxfrd*, que melhora a performance da replicação pela cópia direta dos arquivos dbm. Entretanto, o *ypxfrd* não suporta a replicação entre sistemas utilizando sistemas operacionais diferentes (ex. Linux x Solaris) ou processadores diferentes (ex: Linux em PC x Linux em Mac).

O servidor slave pode perder atualizações enviadas pelo master (por exemplo, se estiver desligado), por isso é recomendado executar o comando *ypxfr* periodicamente via *cron* para atualizar o slave. A maioria das distribuições já faz isso por default.

clientes NIS, de modo que pode-se ter ao mesmo tempo usuários da rede (fornecidos pelo NIS) e usuários locais (fornecidos pelo diretório */etc*).

Não é desejável incluir usuários como root, bin, adm, ftp news e outros usuários de serviço no NIS, pois isto pode levar a problemas de configuração em servidores diferentes. O valor 500 é apropriado para a maioria das distribuições, em caso de dúvida observe o menor UID de usuários regulares em seu sistema.

Montagem de cliente NIS

Agora que você tem um servidor NIS no ar, pode configurar uma estação como cliente. Devem ser instalados os pacotes *ypbind*.rpm* e *yp-tool*.rpm*. Depois edite o arquivo */etc/yp.conf* para incluir a linha:

```
domain pcmaster broadcast
```

Ela faz com que qualquer servidor NIS presente seja localizado e utilizado. Ou então:

```
domain pcmaster server hostname
```

Onde hostname é o nome (presente no arquivo */etc/hosts* ou resolvido por DNS) do servidor NIS. Pode-se ter várias linhas desta segunda forma caso existam servidores slave na rede.

Iniciamos o cliente NIS com um dos comandos abaixo:

```
service ypbind start
/etc/rc.d/init.d/ypbind start
```

Observe que a maioria das distribuições do GNU/Linux configura por padrão um firewall ipchains ou iptable, que poderá estar bloqueando o acesso ao servidor *ypserv*. Inicie os testes com o NIS desabilitando todas as regras de firewall no servidor NIS:

```
ipchains -F
iptables -F
```

Mais tarde veremos como lidar com NIS em servidores que rodem um firewall.

Você pode testar o funcionamento do cliente NIS utilizando os comandos:

```
ypwhich
ypcat hosts
```

O primeiro indica a qual servidor NIS o cliente está conectado, e o segundo exibe o conteúdo do banco de dados de hosts (*/etc/hosts*) fornecido pelo servidor NIS.

Inicializando o NIS durante o boot do GNU/Linux

Pode-se incluir o comando *nisdomainname* em um dos scripts de boot do sistema (*/etc/rc.d/**) ou em sistemas que utilizam o */etc/sysconfig*, como o Red Hat Linux. Basta editar o arquivo */etc/sysconfig/network* e acrescentar a linha:

```
NISDOMAIN=pcmaster
```

O comando *ntsysv*, ou qualquer outro front-end administrativo, pode ser utilizado para iniciar os *dameons* durante o boot do sistema. Pode-se também utilizar os seguintes comandos:

```
chkconfig ypserv on
chkconfig yppasswdd on
chkconfig ypxfrd on
chkconfig ypbind on
```

Atualização do Banco de Dados do NIS

Qualquer modificação em um dos arquivos no diretório */etc* que servem como base para a geração dos bancos de dados, como a criação de novos usuários, implica em executar novamente o Makefile no diretório */var/yp*:

```
make -C /var/yp
```

Este tipo de ação é facilmente configurada no Webmin ou no Linuxconf, mas haverá um problema quando usuários regulares modificarem suas senhas.

O comando *passwd* padrão é capaz de atualizar apenas o arquivo */etc/passwd* (ou */etc/shadow*) local, não sendo capaz de realizar a atualização no servidor NIS. Para que um usuário possa modificar a sua senha, existe o comando *yppasswd*, que se comunica com o *daemon yppasswdd* ativo no servidor NIS master e faz a atualização da senha. Muitos administradores substituem o comando *passwd* padrão pelo *yppasswd* para facilitar a vida dos usuários.

Em versões mais antigas do Red Hat o *yppasswdd* era fornecido em um pacote separado, mas versões atuais o incluem no pacote *ypserv*.rpm*, de modo que basta iniciá-lo depois do *ypserv*:

```
service yppasswdd start
/etc/rc.d/init.d/yppaswd start
```

Em algumas distribuições pode ser necessário editar o arquivo */etc/nsswitch.conf* para incluir a opção *nis* ao menos nas entradas *passwd*, *shadow* e *group*.

O NIS é baseado em RPC, de modo que o *daemon portmap* também deve estar rodando para que um cliente ou servidor NIS possa ser ativo. A maioria das distribuições instala e inicializa o *portmap* por default, pois ele também é utilizado pelo NFS.

Finalmente, é bom lembrar que na configuração padrão do NIS deve-se desativar qualquer firewall ativo nos servidores *master* e *slave*.

Segurança e NIS

O NIS tem a fama de não ser um serviço muito seguro. Parte desta fama vem de uma série de exploits sobre os *daemons yp** ou sobre o *portmap* que foram identificados e sanados há mais de 10 anos. Mas parte disto também vem do fato de não existir no NIS nenhum recurso de autenticação dos computadores envolvidos no domínio. A solução para este problema seria utilizar o NIS apenas para fornecer profiles e o Kerberos para autenticação.

Além disso, o mecanismo padrão de autenticação por *login/senha* é sujeito a ataques de replay (por isso o Windows utiliza *chalenge/response* em versões mais recentes).

O banco de dados de senhas no NIS está acessível a todos os usuários em qualquer nó da rede, de modo que podem ser utilizados crackers de senhas, anulando o ganho de segurança fornecido pelo arquivo */etc/shadow*.

É possível configurar serviços baseados em RPC e em particular o NIS para utilizar comunicação criptografada baseada em certificados digitais e chave pública/privada, garantindo segurança. Porém, o uso de criptografia não é suportado pelo NIS em alguns sistemas Unix like.

Outra dificuldade com o NIS é que é preciso desligar o firewall nos servidores *master* e *slave*. A configuração normal de aplicações baseadas em RPC utiliza números de porta dinâmicos, fornecidos aleatoriamente pelo *portmap*, de modo que não se sabe a priori quais portas abrir no firewall.

Todos os *daemons* do NIS suportam a opção *-p*, que permite especificar um número de porta para o serviço. Para incluir esta opção deve-se editar os scripts de inicialização de cada *daemon* no diretório */etc/rc.d/init.d*. Cada *daemon* deve ter a sua própria porta e, além disso, deve-se liberar a porta 111 (*sunrpc*) para acesso ao *portmap*.

Versões mais recentes do NIS não suportam *tcpwrappers*, mas pode-se utilizar os arquivos */var/yp/securenets* ou */etc/ypserv.conf* para estabelecer restrições de acesso baseadas em endereços IP.

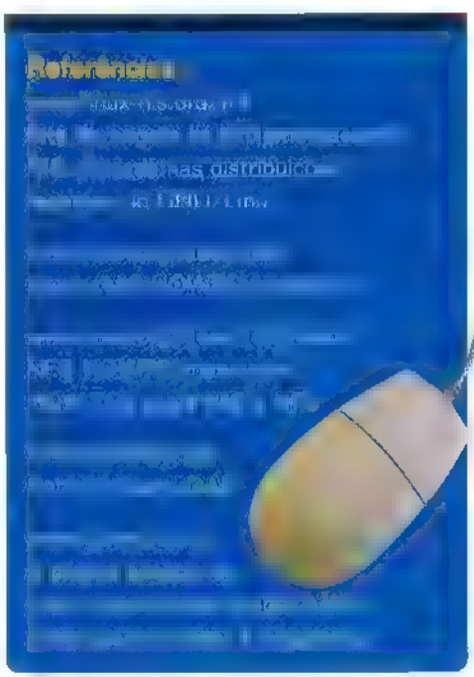
Considerações finais

Uma solução de integração de usuários em redes Unix ou Linux utilizando NIS (ou qualquer outro mecanismo) depende de um serviço de compartilhamento de arquivos, pois a maioria dos aplicativos armazena suas configurações particulares em arquivos escondidos armazenados no diretório home do usuário.

Em geral utiliza-se o NFS, e um único servidor de arquivos fornece o diretório */home* para todos os servidores e estações da rede. Lembre-se de liberar a porta 2049 (nfs) se o servidor de arquivos rodar algum firewall. É uma boa idéia utilizar *rdist* ou algum outro mecanismo de replicação de arquivos para ter uma cópia standby dos diretórios *home* dos usuários.

O NIS, apesar das suas deficiências de segurança, é perfeitamente adequado a redes pequenas e médias, mas ainda assim, é a melhor solução, já que sistemas muito usados anteriormente, como o NT ou o Netware 3.x, também apresentavam deficiências similares.

Além disso, ao contrário do NIS, o uso de sistemas mais seguros como LDAP ou Kerberos não resolve problemas mais sérios como senhas triviais ou bugs que permitem ataques de buffer overflow e exigem uma curva de aprendizado bem mais longa. **PCM**



Artigo

O especialista

Eles sabem o que falam. Todo mês uma superdica completa, escrita por um profissional da área, mostrando uma solução para seus problemas

Alta Disponibilidade

Esse tema tem despertado muito interesse e aqui você vai verificar os conceitos, suas vantagens e desvantagens, além de alguns exemplos práticos usando sistema Linux

Por Sulamita Garcia

A disponibilidade é definida como a probabilidade de um sistema estar disponível (em perfeito funcionamento) em dado momento. E a pode ser classificada como:

- **Básica:** qualquer sistema disponível no mercado garante uma disponibilidade de 99%.
- **Alta:** sistemas mais especializados, que garantem soluções "de alguns noves" (99,99%, 99,9999%). As empresas brigam para ver qual adiciona mais noves à sua solução.
- **Contínua:** situação ideal, mas teórica. A disponibilidade é igual a 1, ou seja, o sistema está sempre disponível. Infelizmente, é apenas hipotética. Embora seja possível garantir muitos noves, sempre existe uma possibilidade do sistema parar.

Ficha da autora

Sulamita Garcia, anal[illegible]
Fast Pack – www.fastpack.com.br
Contato: sulamita@fastpack.com.br

Aumente a disponibilidade

Existem várias formas de tentar contornar-se as falhas dos sistemas computacionais e aumentar a disponibilidade. Alguns exemplos são:

- **Hardware especializado:** existem no mercado várias alternativas de hardwares mais especializados que preveêm uma possível falha, tratando isto com redundância de recursos. Outros são voltados para a disponibilidade, com softwares que executam balanceamento de carga, redundância de links, tomada de serviços, monitoração e backup em tempo real, entre outras coisas. Mas tais sistemas, quanto mais especializados, mais expansivos são. E também têm um poder computacional muitas vezes bem maior do que o necessário.
- **Sistemas de tolerância a falhas:** aplicativos que evitam que falhas se tornem erros, e erros se tornem defeitos. Falhas dizem respeito ao universo físico, quando há, por exemplo, interferência eletromagnética. Erros ocorrem quando estas falhas mudam o valor de algum dado, como trocando o valor de algum bit. A melhor maneira de se tratar um problema é logo no começo dele, na hora em que é causado, evitando danos maiores, como corrupção e/ou perda de dados. Porém, sistemas assim são extremamente trabalhosos e complexos de serem desenvolvidos, requerem um profundo e especializado conhecimento, além de serem aplicações pesadas.
- **Alta disponibilidade:** prevê a redundância total do sistema, atuando em caso de defeito, quando a máquina trava. Isto é chamado defeito, onde um erro causa uma pane no sistema, afetando o universo do usuário. Trabalha com a hipótese de completa parada do sistema através de uma solução em redundância de hardware e controle via software. Um sistema de alta disponibilidade prevê tal comportamento com hardware simples, deixando a complexidade e o controle da disponibilidade do sistema para o software.

Gerenciamento

Para um bom desempenho de um ambiente usando uma solução de alta disponibilidade, é necessário o planejamento de uma estratégia de

Exemplo de uma solução

Para uma solução utilizando Linux foi usada a combinação de *ext3+drbd+heartbeat+mon*. Acompanhe:

- **Sistema de Arquivos Journaled Ext3:** talvez o *Reiserfs* seja mais utilizado mas o *ext3* oferece a compatibilidade com o *ext2*, eliminando a necessidade de se recriar o *filesystem*. Existe uma superioridade do *Reiserfs* sobre o *Ext3* mas é tão pequena que não supera a facilidade e a segurança na mudança

- **Espelhamento de dados – DRBD:** o *DRBD* (Distributed Replicated Block Device) espelha os dados em blocos repassando-os através da rede. Funcionando em pares, ele estabelece em cada nodo uma partição para espelhar, e seta um dos nodos como primário. Toda alteração irá ser refletida no secundário. O primário tem a partição com *DRBD* montada, já o secundário não.

- **Sinal de Vida – Heartbeat:** onde reside a configuração dos serviços e do IP de serviço. O *heartbeat* é o responsável pela reconfiguração automatizada na ocorrência de problemas. Cada máquina possui seu IP próprio, válido ou não, mas o conjunto é identificado por um IP de serviço mantido pela máquina primária no par. Em caso de pane no sistema o *heartbeat* de um lado libera os serviços e IPs e do outro assume

- **Mon:** bastante leve, possui diversos monitores e sistemas de alerta para as mais variadas funções e serviços. Possui envio de mensagens via página, correio, sms e pode ser configurado para disparar programas em qualquer linguagem

Num quadro geral, o Mon ficaria monitorando o sistema. Ao detectar que um serviço não está respondendo, que a máquina está com pane, que está isolada da rede (no nodo primário), ou que o nodo secundário não está respondendo, ele dispararia o *heartbeat* para derrubar ou para levantar os serviços. Um destes serviços deve ser o *DRBD*, que embora sempre espelhando não estaria com a partição montada. Montando estas partições com os dados atualizados para o serviço que se oferece, estes serviços estarão em condições de responder com autoridade para os usuários

gerenciamento. Uma análise primária deve identificar o que é envolvido neste ambiente, como:

- Um conjunto de recursos e estados destes recursos a serem gerenciados
- Uma coleção de testes executados periodicamente e/ou sob comando
- Um conjunto de ações a serem tomadas quando os testes falharem
- Um conjunto de ferramentas para observar e gerenciar os recursos

Estes componentes devem trabalhar juntos para gerenciar o ambiente e são o ambiente em si. Veja exemplos de recursos ou estados a serem gerenciados:

- Um servidor HTTP
- A conectividade com um determinado host
- O estado de uma placa de rede
- O estado de um hub ou switch
- Uma unidade de armazenamento

Ações que podem ser tomadas:

- Reinício do serviço HTTP
- Reinício da máquina
- Reconfiguração de outra máquina para tomada do endereço IP
- Reconfiguração de rotas para contornar um equipamento que não responde
- Notificação do administrador do sistema via e-mail, pager

Configuração do ambiente

Conseguimos este ambiente de alta disponibilidade com a redundância de hardware, tendo uma máquina chamada de nodo – principal e outras secundárias, que seriam como espelhos do nodo principal

Para que uma máquina espelho assuma o lugar quando a principal falhar, ambas devem possuir os mesmos dados e/ou recursos envolvidos no tipo de serviço oferecido.

Veja o que envolve a montagem de um ambiente de alta disponibilidade:

- **Hardware:** redundância de máquinas (requisito), de links, conexão dedicada e de alta velocidade (recomendada)

- **Instalação do sistema:** os softwares devem ser independentes de distribuição. A identidade das máquinas, quem será o principal e quem será o espelho, fica a cargo do administrador do sistema.

- **Consistência dos dados:** sistemas de arquivo *journaled*. Estes sistemas armazenam em um journal (log) as ações antes de serem efetuadas. Desta forma, em uma parada no sistema, seja por pane no sistema ou queda de energia, a recuperação é muito mais rápida e indolor

- **Espelhamento de dados:** os dados devem ser espelhados em tempo real para a completa disponibilidade do sistema em caso de defeito

- **Controle de serviços:** com os dados espelhados, os serviços podem ser passados de uma máquina para outra. Porém o sistema deve ser autônomo nesta transferência e capaz de se reconfigurar para continuar atendendo aos usuários.

- **Monitoração:** o sistema deve monitorar seus serviços para detectar um defeito, disparando assim a reconfiguração.

Para maiores detalhes de como implementar este ambiente, veja no site http://ha.underl.nux.com.br/ um *how to* com todos os passos para a instalação e configuração de tal ambiente. **PCM**

Falhas de SEGURANÇA

Confira as principais falhas de segurança do último período e aprenda como resolvê-las. Os arquivos comentados estão em www.europanet.com.br/pcmaster/edicao66

Por Domingo M. Montanaro

OpenSSL + Apache

Sistema Operacional: FreeBSD
Tipo: Remota / Local
Versões Afetadas: Apache: 1.3.26, 1.3.19. OpenSSL: 0.9.6. FreeBSD 4.4-STABLE até 4.6-RELEASE-p1
Nível: Avançado
Gravidade: Alta
Privilégios: Acesso remoto à conta do Apache

Descrição:

O OpenSSL é um pacote de ferramentas para a implementação do protocolo SSL (Secure Sockets Layer) e TLS (Transport Layer Security – também conhecido como SSL v2/v3), além de ser utilizado como uma biblioteca de criptografia. Em sua implementação com o Apache, ele possui uma falha de buffer não verificado no qual é possível à um atacante sobrescrever um endereço de memória e assim obter o acesso ao sistema alvo com privilegios do servidor Apache

Como explorar:

Faça o download do exploit, compile e rode *openssl-bsd.c*. Para isso use o comando a seguir:

```
$ gcc -o openssl openssl-bsd.c -
lcrypto
$ ./openssl  <-h hostname> [-t
arch] [-p port] [-c N] [-b
0x<address>][-brute]
```

Como Explorar:

Instale o Patch *OpenSSL.patch* disponível em www.europanet.com.br/pcmaster/edicao66, ou atualize o OpenSSL para a versão 0.9.6e.

IBM WebSphere

Sistema Operacional: Windows 2000 Server
Tipo: Remota
Versões Afetadas: 4.0.3
Nível: Intermediário
Gravidade: Alta
Privilégios: Indisponibilização do sistema

Descrição:

O WebSphere é um software de Infra-Estrutura de Internet, muito utilizado como servidor de aplicações, que contém uma falha de segurança ao tratar uma grande requisição HTTP Ao requisitar um arquivo com extensão *jsp*, mesmo sem existir no servidor, é possível que o mesmo pare de responder, se no campo *HOST* do cabeçalho HTTP existir uma string com mais 796 bytes.

Como explorar:

Efetue uma conexão HTTP à máquina-alvo, e envie uma requisição HTTP completa, sendo que no campo *HOST* exista uma string com 796 caracteres

Como proteger:

Baixe o patch disponibilizado pela IBP em http://www-1.ibm.com/support/docview.wss?rs=180&context=SSEQTP&q=PQ62144&uid=swg24001610.

Apache TomCat

Sistema Operacional: Todos
Tipo: Remota
Versões Afetadas: 4.0.4, 4.1.10
Nível: Básico
Gravidade: Média
Privilégios: Visualização de códigos

Descrição:

O TomCat é um aplicativo usado em conjunto com o Apache para implementar ambientes baseados em ServLets Java. Quando é requisitado o *ServLet default* com *org.apache.catalina.servlets.DefaultServlet*, a falha permite que o código-fonte do arquivos JSP no servidor seja exibido em seu navegador Internet.

Como explorar:

Para visualizar o documento efetue uma requisição HTTP na máquina-alvo pelo endereço: http://endereco/servlet/org.apache.catalina.servlets.DefaultServlet/documento.jsp.

Como Proteger:

Faça o download da nova versão (estavam disponíveis a 4.0.5 e 4.1.12) do Apache TomCat no endereço http://jakarta.apache.org/builds/jakarta-tomcat-4.0/release/.

/bin/login

Sistema Operacional: Solaris, SunOS
Tipo: Remota / Local
Versões Afetadas: SunOS SPARC 5.5, 5.5.1, Solaris SPARC 2.6, 2.7 e 2.8 || SunOS x86 5.7 e 5.8
Nível: Avançado
Gravidade: Alta
Privilégios: Acesso à conta de qualquer usuário

Descrição:

Existe um problema de buffer não verificado quando o */bin/login* verifica a variável de ambiente TTYPROMPT. Esta vulnerabilidade já havia sido reportada e a Sun havia disponibilizado uma correção, mas a vulnerabilidade persiste se a variável TTYPROPT for definida dentro da aplicação *telnet*. Desta maneira, é possível à um atacante simplesmente logar no sistema com qualquer login, inclusive root, uma vez que o sistema-alvo tenha habilitado o login do usuário root por telnet.

Como explorar:

Existem duas maneiras, manualmente e com exploit. Para fazer manualmente, entre no telnet e defina a variável TTYPROMPT com um valor qualquer de 6 caracteres.

```
$ telnet
telnet> environ define TTYPROMPT edsono
```

Conecte se ao sistema-alvo:

```
telnet> o SISTEMA-ALVO
```

Após eventuais banners, o login será requisitado. Basta digitar o login desejado seguido de 64 vezes a sequência " ", ou seja, um espaço mais os caracteres de quebra de linha \n. Após isso, seu login será efetuado sem o pedido de senha.

Usar o exploit é ainda mais simples:

```
$ gcc -o login sunlogin.c
$ ./login -u USUARIO -p porta -h sistema alvo
```

Como Explorar:

Faça download e instale o patch disponibilizado pela Sun em http://sunsolve.sun.com.

Cisco VPN 5000

Sistema Operacional: Linux e Solaris
Tipo: Local
Versões Afetadas: Linux, 5.2.7 Solaris, 5.2.8
Nível: Avançado
Gravidade: Alta
Privilégios: Usuários locais podem obter privilegios de Super Usuário

Descrição:

O Cliente do Cisco VPN 5000 rodando em Linux e Solaris possui uma falha de Buffer Overflow em dois de seus binários, *close_tunnel* e *open_tunnel*, que são *setados* uid root como padrão. Esses programas, durante sua execução, copiam argumentos da linha de comandos para buffers estáticos de memória, que não são verificados, deixando assim a aplicação vulnerável. Isso permite o acesso ao sistema com permissão de super usuário.

Como explorar:

Somente poderá ser executado por usuários que tenham acesso ao sistema que será explorado. Para isso, logue com seu usuário na máquina-alvo e compile o exploit *ciscovpn.c*:

```
$ gcc -o ciscovpn ciscovpn.c
```

Apenas execute o arquivo compilado e você terá privilégios de super-usuário no sistema. Para isso, digite o comando:

```
./ciscovpn
```

Como Proteger:

Baixe a última versão do Cisco VPN Client em http://www.cisco.com/univercd/cc/td/doc/product/aggr/vpn5000/client/.

Domingo M. Montanaro
[illegible]

PCM

Família

Converse sobre Linux com outros usuários. São milhares espalhados em diversos grupos. Todos eles com um interesse em comum: aumentar o seu conhecimento sobre o sistema operacional que vem conquistando mais espaço a cada dia.

E para que você possa fazer parte deste universo, publicamos a seguir uma lista de vários grupos de usuários Linux brasileiros. Basta escolher um deles e fazer o cadastro para ficar por dentro das últimas novidades.

Linux Hangar
www.linuxhangar.hpg.com.br

SERVUX - Servidores Linux
www.servux.cjb.net

Segurança no Conectiva Linux
distro.conectiva.com.br/mailman/listinfo/seguranca

AnO2001
www.ano2001.com

Prog-BR - Programação Linux
listas.conectiva.com.br/listas/

LDP-BR Projeto de Documentação Linux
ldp-br.conectiva.com.br

JustLinux
groups.yahoo.com/group/justlinux

GUS – Grupo de Usuários Slackware
gus-br.linuxmag.com.br

Grupo de Discussão Linux
groups.yahoo.com/group/linux-board

Grupo de Usuários Linux do Vale do Taquari
mercurio.fates.tche.br/linux/

Nosso Grupo - Sistemas
www.nossogrupo.com.br/canais.asp?canal=275

Linuxabc
linuxabc-subscribe@egroups.com

Linux-br
linux-br.conectiva.com.br

Grupos Brasileiros

1 - PARÁ
Linux em Belém do Pará
br.groups.yahoo.com/group/linuxparadegua

Linux - Pará
www.linux-pa.org

2 - MARANHÃO
Comlinux - Comunidade Linux do Maranhão
www.comlinux.ufma.br

3 - CEARÁ
Linux-CE - www.ibeuce.net/lists/linux-ce

4 - RIO GRANDE DO NORTE
Universidade Federal do RN
ufrn.br/servicos/lista_discuss.html

Grupo de Usuários Linux do Rio Grande do Norte
www.linuxpotiguar.tsx.org

5 - PARAÍBA
GLUG/PB - Grupo de Usuários GNU
www.glugpb.cjb.net

Linux-Sever
http://linux.sathi.com.br

6 - PERNAMBUCO
Grupo de Usuários GNU/Linux de Pernambuco
www.glugpe.cjb.net

7 - SERGIPE
Linux Sergipe
linux-se-subscribe@egroups.com

Linux-SE Grupo de Usuários Linux de Sergipe
come.to/linux-se

8 - BAHIA
GULBA - Grupo de Usuários Linux da Bahia
www.gulba.org

Clube de Usuários Linux World Bahia
www.geocities.com/Eureka/Gold/2399

9 - MINAS GERAIS
Linux BH
www.linuxbh.cjb.net

Grupo de Usuários GNU/Linux de Juiz de Fora
linuxjf.jfnet.com.br

BLUG - BHZ Linux Users Group
blug.tsx.org

BHNET - Linux
www2.bhnet.com.br/lista-linux

LinuxBQ - Barbacena Querida
www.linuxbq.org

Centro de Treinamento e Serviços Linux de MG
www.comunidadelinux.com.br

Comunidade Neurix
www.neurix.com.br

GNU\LinuxMG
irc.brasirc.net - #LinuxMG

10 - ESPÍRITO SANTO
Grupo de Usuários Linux do Espírito Santo
www.linuxes.com.br

Grupo de Usuários Linux - ES
www.inf.ufes.br/~linux

11 - RIO DE JANEIRO
Linux Resende
linux-resende-subscribe@egroups.com

Grupo da Cidade de Três Rios
www.nossogrupo.com.br/grupo.asp?grupo=7852

Gral- Grupo de Estudos Avançados Linux
gral.stat.com.br

GULSF - Grupo de Usuários Linux da Região Sul Fluminense
www.linuxbr.info

Grupo de Usuários GNU Linux de Volta Redonda
www.linuxvr.hpg.com.br - linuxvr@eg.com.br

Linux

Participe de um grupo de usuários Linux. No Brasil existem dezenas de grupos onde você consegue trocar experiências e saber mais sobre o sistema

Meu Grupo Sistemas Operacionais
www.meugrupo.com.br/SubCategoria.cfm?ID_SubCategoria=3

LinuxAll.org
www.linuxall.org - Edson Syguedomi
webmaster@linuxall.org

Linux - Alta Disponibilidade
l nux-ha-br-subscribe@bazar.conectiva.com.br

Grupos de usuários de Linux do Norte/Nordeste
www.nordestelinux.rg3.net

LinuxBQ - Linux ao alcance de todos!
www.l nuxbq.cjb.net

Cipsga - Comitê de Incentivo à Produção de Software Gnu e Alternativo
www.cipsga.org.br

StarNux
www stanux hpg com br

Linux na Rede
www.linuxnarede.hpg.com.br

Linux Clube
www.linuxclube.com

GRUPO DO MÊS

Grupo de Usuários da Biologia – USP

http://www.cybershark.net

Formado por usuários interessados em informática em geral mas em especial o L nux, no início do grupo os integrantes cursavam b o logia na USP Vem desenvolvendo a troca de experiência através de e-mail e muito mais

VOCÊ TEM UM GRUPO?

Se você conhece algum grupo de usuários Linux que não esteja nesta lista, envie para o e-mail pcmaster@europanet.com.br.

LUG-Petrópolis
Linux User Group Petrópolis
petropolis.lug inf br

LUG-RIO
Linux User Group Rio de Janeiro
rio lug inf br

12 - SÃO PAULO
Grupo de Usuários Linux de Sorocaba
www.guls.com.br

Linux-L
inux unesp br

GULIB
Linux da Biologia/USP
www.cybershark.net

LinuxSP
www linuxsp org.br

Grupo de Usuários Linux IME
gu linux me.usp br

Rizl Comunidade Linux de Matão
linux.process.com.br

Guia Tecnológico Free-Soft
www linux.unesp br

Comunidade Linux
www.coml nux com.br

13 - PARANÁ
Linuxer de Curitiba - PR
www nuxercenter.cjb.net

14 - SANTA CATARINA
GU LINUX FLORIPA
www inux-sc org

15 - RIO GRANDE DO SUL
Grupo Linux de São Leopoldo
www sl nux hpg g com br

G.U. Linux de Erechim
www.geocit es com/gu elinux

GU Porto Livre
www portolivre.org

GNUTeen - Grupo de Usuários Linux de Candiota
www gnuteen hpg g.com br

Gnurias
www.univates br/gnurias

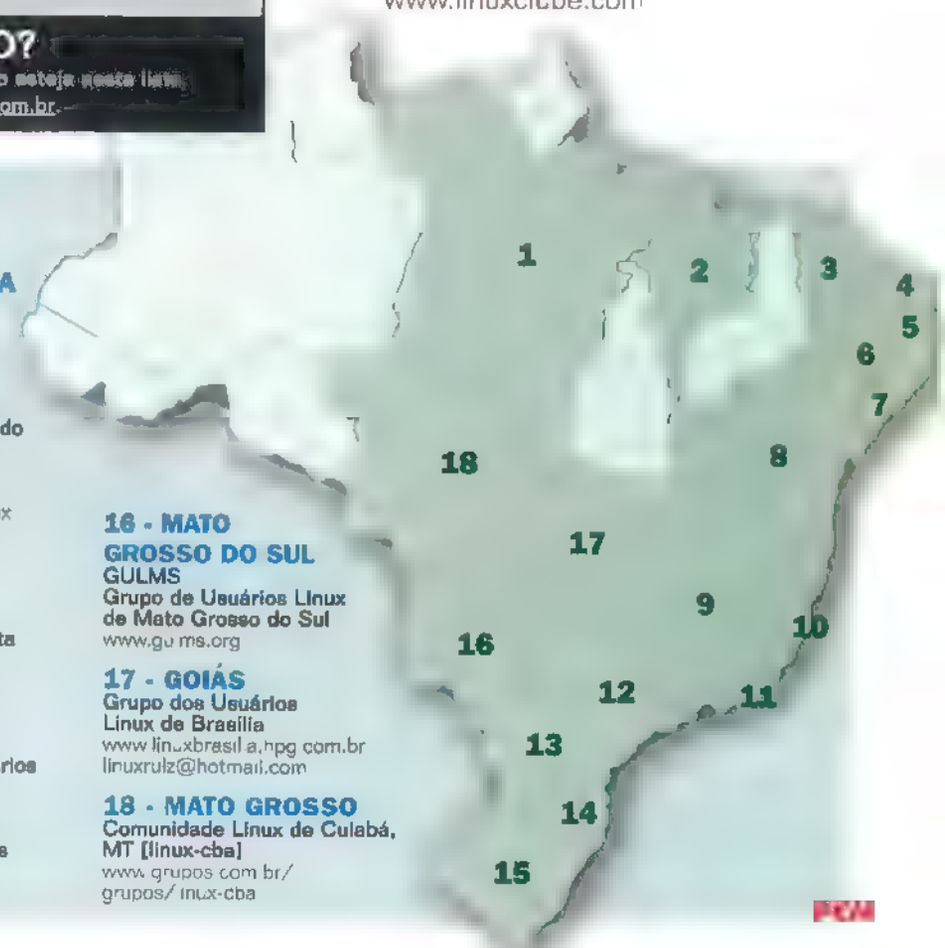
TaquariX - Grupo de Usuários do Vale do Taquari
www.un vates br/ taquarix

GULP - Grupo de Usuários Linux de Pelotas
http://gulp.ucpe tche.br

16 - MATO GROSSO DO SUL
GULMS
Grupo de Usuários Linux de Mato Grosso do Sul
www.gu ms.org

17 - GOIÁS
Grupo dos Usuários Linux de Brasília
www linuxbrasil a.hpg com.br
linuxrulz@hotmail.com

18 - MATO GROSSO
Comunidade Linux de Cuiabá, MT [linux-cba]
www grupos com br/grupos/ inux-cba



HelpLine

Aproveite este espaço e esclareça suas dúvidas sobre Linux, Windows e Informática em geral

Por Rodrigo Galan
helpline@europanet.com.br

Num Lock na Inicialização

Instalei o Conectiva, mas ao inicializar o sistema a função da tecla Num Lock não fica ativa. Existe algum comando que ative esta tecla na inicialização ?

Amilton de Serrad
Via Internet

Sim, em algumas distribuições como a Conectiva esta função vem desmarcada, mas é possível ativá-la alterando o arquivo rc.sysvinit. Para isso, entre com um editor de texto e abra este arquivo em /etc/rc.d/rc.sysvinit. Agora, adicione os seguintes parâmetros:

```
for tty in /dev/tty[1-9]*; do
/usr/bin/setleds -D +num <
$tty done
```

Salve este arquivo e reinicie o PC

Backup com permissão

No Linux, a pasta */home* contém todos os arquivos dos usuários cadastrados e cada usuário tem diferentes tipos de arquivos com as suas devidas permissões. Como faço um Backup em um outro HD mantendo as suas permissões?

Josevaldo Xavier
Via Internet

Uma maneira de copiar os arquivos mantendo as permissões é utilizar um procedimento pouco conhecido, mas bastante eficiente devido à velocidade em que os arquivos são copiados

Entre no Console ou no Shell e digite o comando:

```
(cd /origem/diretório && tar cf - . ) |
(cd /destino/diretório && tar xvfp -)
```

Arquivos de configuração

Sempre que preciso encontrar o local onde estão os arquivos de configurações de alguns programas, utilizo o comando *Find*, mas a busca acaba sendo demorada. Existe algum programa que faça uma busca mas que mostre o local onde estão os arquivos sem precisar fazer uma varredura como acontece com o comando Find?

Silvana Cardoso
Via Internet

Sim. Um excelente método para encontrar arquivos de configurações, pastas e até o próprio programa executável é utilizar o comando whereis. Para isso, digite no console ou Shell:

```
# whereis samba
```

Onde samba é o arquivo ou pasta que deseja localizar

Removendo programas

Desinstalei um programa pelo ícone que estava dentro da pasta no menu Iniciar, mas o programa continua na lista de Adicionar ou Remover Programas. Mesmo removendo o programa pelo Adicionar ou Remover Programas ele ainda continua na lista. Teria alguma forma de remover o programa da lista?

Nilson Garcia
Via Internet

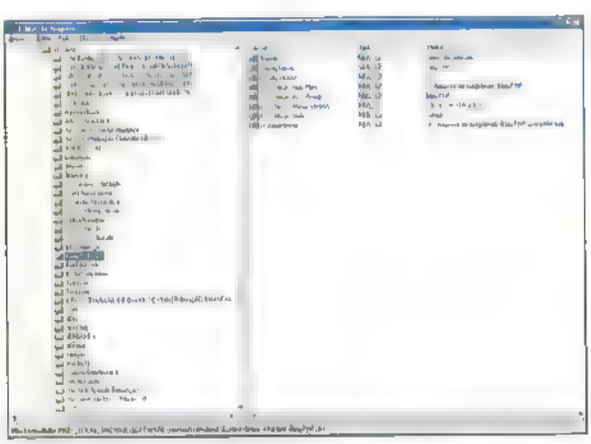
Sim, para fazer isso é necessário utilizar o Editor de Registro do Windows. Siga o seguinte procedimento.

1 *Clique em Iniciar. Em seguida, clique em Executar e digite*

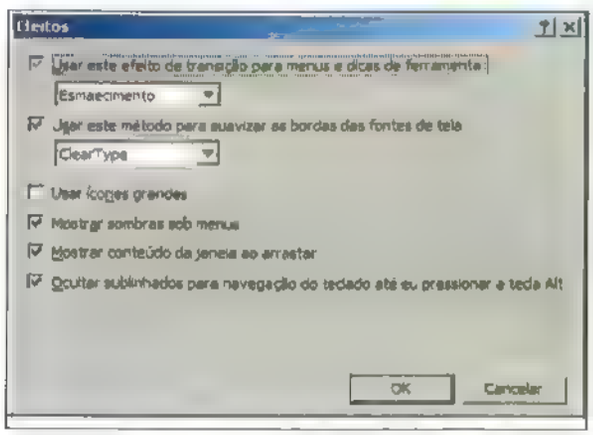
```
Regedit
```

E clique no botão Ok

2 *Dentro do Regedit acesse:* HKEY_LOCAL MACHIN\Software\Microsoft\Windows\Current Version\Uninstall



Para remover arquivos da lista Adicionar e Remover Programas, utilize o Editor de Registro do Windows



A opção ClearType permite suavizar as fontes do Windows e tornar a leitura menos cansativa

3 *Dentro da pasta* Uninstall *aparece uma lista de pasta com os nomes dos programas instalados no computador. Para remover um programa da list, basta remover a pasta correspondente para que seu nome não apareça mais no Adicionar ou Remover Programas*

Fontes suaves no Win XP

No Windows XP em que trabalho as fontes são suaves, como se estivessem borradas, mas no Win XP da minha casa as fontes são normais. Como colocar as fontes suaves no meu computador?

Alexandre Pereira
Via Internet

Este recurso é pouco usado mas bastante eficiente pois deixa as fontes mais legíveis, tornando a leitura menos cansativa. Para modificar o parâmetro das fontes, clique com o botão direito do mouse sobre o Desktop. No menu que irá surgir, clique na opção Propriedades. *Na janela* Propriedades de Vídeo *entre na aba* Aparência *e clique no botão* Efeitos *Marque a opção* Usar este método para suavizar as bordas das fontes na tela. *Na lista suspensa selecione a opção* ClearType, *clique em Ok e em Ok novamente*

Fila de impressão

Eu tenho um servidor de impressão que está compartilhado diretamente com o Samba. Quando deseo remover algum trabalho que está na lista tenho que reiniciar o computador para cancelar a impressão. Como faço para cancelar os trabalhos na fila de impressão sem precisar reiniciar o computador?

Evandro Gonçalves
Via Internet

Remover os trabalhos de impressão é muito simples. Normalmente utilizamos o comando lprm. *Para cancelar todos os processos sem verificar quantos estão na lista digite no console.*

```
# fuser -k /dev/lp0
```

Onde lp0 *é a porta onde a impressora está conectada. É possível também utilizar este comando para impressoras conectadas na porta USB:*

```
# fuser -k /dev/usb p0 ou fuser -k
/dev/usb/ p0
```

Para saber quantos processos então esperando para ser impressos basta digitar:

```
# lpc status ou lpc all
```

E para a fila de impressão digite:

```
# lprm -Pall a l
```

Arquivos RPM no Slackware

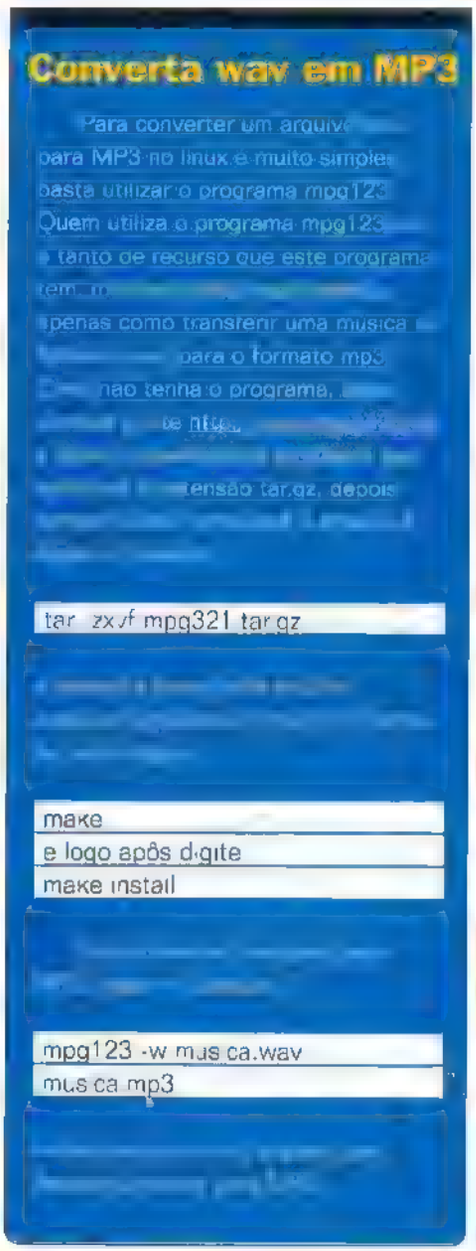
Tenho instalado em meu computador o Linux Slackware, mas tenho um sistema baseado em pacotes RPM. Como faço para instalar pacotes RPM no Slackware?

Ademir Correia
Via Internet

No Slackware os pacotes suportados são os tgz e tar.gz, para instalar pacotes do tipo RPM (RedHat Package Manager) é preciso antes convertê-los para um pacote que seja suportado pelo Slackware Utilize o comando rpm2targz *e faça o seguinte procedimento:*

1 *No local onde está o arquivo RPM faça o seguinte comando.*

```
# rpm2targz
nomedoarquivo.rpm
```



Onde nomedoarquivo é o nome do arquivo que você deseja converter para tar.gz

2 *Agora, converta este arquivo para tar.gz. para isso digite*

```
# rpm2tgz
nomedoarquivo.tar.gz
```

Onde nomedoarquivo é o nome do arquivo que deseja converter para tgz.

3 *Para instalar arquivos que têm formato tgz, utilize o comando installpkg. Para isso digite no console:*

```
# installpkg nomedopacote.tgz
```

Imagem ISO no Linux

Tenho uma pasta no Linux que gostaria de transferir para uma imagem ISO. No Windows, são utilizados programas específicos para esta função. Existe também algum comando no Linux que faça a geração de imagem e a gravação?

Jorge da Silva
Via Internet

Sim, para criar a imagem de um diretório, por exemplo, dê o seguinte comando no console:

```
# mkisofs -r -J -o arquivo.iso
/diretório
```

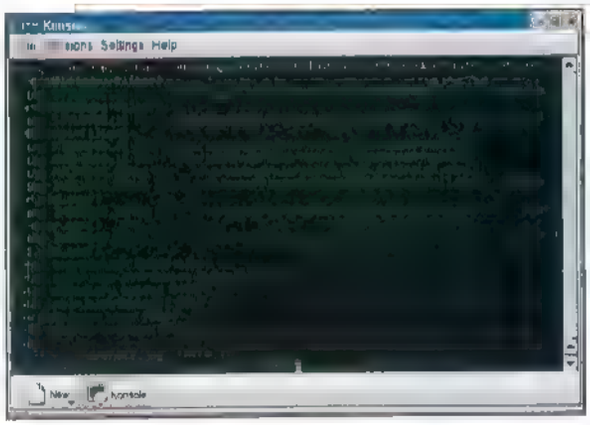
Onde arquivo é o nome da imagem ISO que será gerada e /diretório é o diretório que será copiado para a imagem iso. Veja o seguinte exemplo:

```
# mkisofs -r -J -o arquivos.iso
/var/
```

Para efetuar a gravação da imagem iso no Linux digite o comando:

```
# cdrecord -v -fs=16M
speed=8 dev=0,0,0 -data
arquivo.iso
```

Onde Speed é a velocidade de gravação do CD e arquivo.iso é a imagem que você pretende transferir para o CD



Assim como no Windows, também é possível gerar e gravar imagens ISO no sistema Linux

Login no Debian

Como faço para desligar o login gráfico do Debian?

Alexandre Tarquis
Via Internet

Há duas maneiras de desativar está opção:

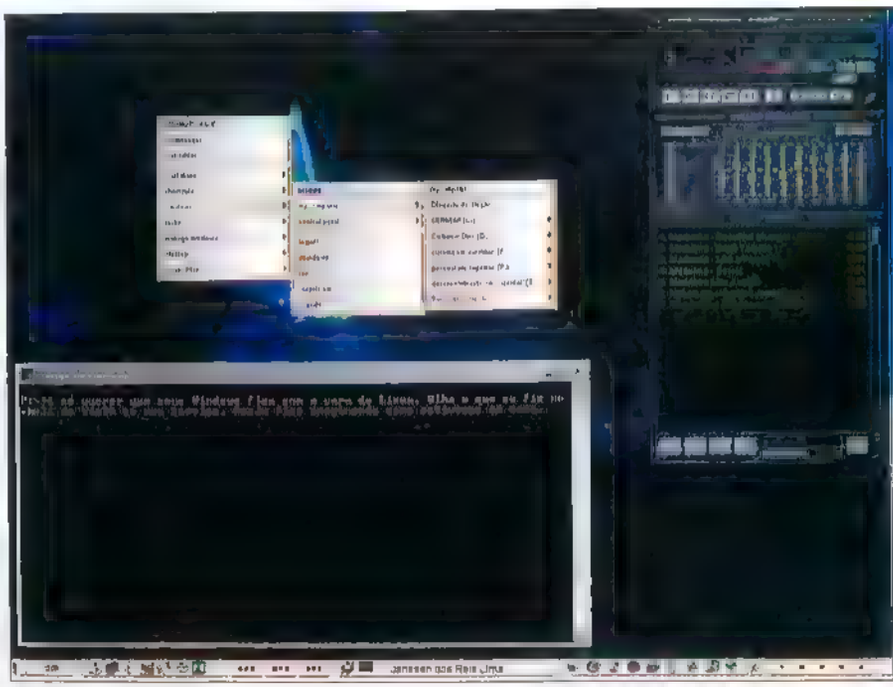
1 *Para impedir que o xdm seja iniciado nos runlevels que esse login gráfico utilizava, digite o seguinte comando no Shell*

```
# update-rc.d -f xdm remove
```

2 *Remova o xdm digitando no Shell o seguinte comando*

```
# apt-get --purge remove xdm
```

Screenshot do Mês



Janssen dos Reis Lima
janssen@sermap.com.br

Windows 2000

Mostre você também a cara [illegible] o seu Desktop para [illegible]

HELPLINE

Se você tem alguma dúvida sobre informática, entre em contato com os nossos especialistas através do e-mail helpline@europanet.com.br. As perguntas mais pertinentes serão respondidas na próxima PC Master.

Seja qual for o destino do seu produto, o ponto de partida é aqui.

Distribuição Sonopress.

A Sonopress dá um completo suporte a seus clientes, oferecendo um leque de serviços cada vez mais eficientes. Através de soluções personalizadas em logística, seus pedidos agora saem direto da fábrica para a mão de seus clientes. Tudo isso, nas quantidades e no mix que você determina.
Sonopress: soluções confiáveis.

Autoração · Replicação de CDs e DVDs
Gráfica · Fulfillment
Distribuição

arvato storage media
A BERTELSMANN COMPANY

Fone: (11) 3613-7300 - Fax: (11) 3611-3364 - www.sonopress.com.br

sono press
Solução na fabricação de CD ROM, Áudio e DVD

www.presenca.com.br

Fazer e Desfazer

O computador é uma máquina do tempo mais poderosa do que se pode imaginar

O primeiro teclado em que pus meus dedos, confesso, não foi o de um computador. As letras estavam lá, sim, todas na posição correta. Também lá estavam os símbolos, a barra de espaço, e mesmo os números, à exceção do 1, que não era necessário. Em conjunto, as teclas formavam uma íngreme rampa que ia do meio do instrumento até a mesa. Tocá-las não produzia qualquer efeito, mas bastava martelar uma das teclas com meus ainda inaptos dedos, para que a letra correspondente aparecesse no papel, após um rápido golpe de alavanca.

O ano era 1989 e eu passava as tardes de minha pré-adolescência – não sou tão velho assim – aprendendo a golpear as duras teclas daquela máquina tão rápido quanto possível. Não é à toa que datilografar e "bater à máquina" eram sinônimos. Era necessário ser rápido, afinal o tempo não pára. Havia, porém, um problema: papel. O papel, capaz de aceitar o "L" minúsculo como número 1 sem reclamar, denunciava, aos berros, cada tecla errada que fosse pressionada, cada linha pulada sem necessidade, cada parágrafo alinhado incorretamente. A grande seta para a esquerda, no canto superior direito do teclado, pouco podia fazer. Voltava-se o espaço de uma letra, é verdade, mas o papel, já marcado, não colaborava. O tempo, enfim, só anda para frente.

O contato com um computador, três anos depois, não podia ter outro efeito que não a fascinação. Quem escreve sabe o que quero dizer. A grande seta, outrora inútil, agora podia apagar as letras recém-digitadas. E havia mais. Era possível apagar e corrigir não apenas trechos recém-escritos, mas qualquer parte de qualquer texto. Era como se o tempo, de repente, tivesse perdido a sua autoridade.

Correções, é verdade, já existiam antes do computador. Mas como tudo na vida, elas deixavam marcas. Marcas que às vezes exigiam que um trabalho fosse refeito. Com um computador, entretanto, os erros podiam ser apagados. Podia-se praticamente voltar o tempo, e não errar. Apesar de ainda ter força nos dedos para martelar a velha máquina de escrever duvido que, após dez anos apagando e desfazendo, eu seja capaz de datilografar uma só folha que preste – ao menos sem gastar um dia inteiro. Graças ao computador foi possível dar asas a uma capacidade humana tão necessária à criatividade quanto a própria inteligência. A capacidade de errar.

E há mais. Além de permitir que corrijamos os nossos erros, o computador tornou-se capaz de lembrar as nossas últimas ações, para que possamos desfazê-las se for conveniente. Basta pressionar algumas teclas. Atrapalhou-se com os dedos? Desfaça. Escreveu alguma besteira? Desfaça. Apagou o que não devia? Desfaça. Perdeu a pessoa amada? Desfaç... É... Bem. Isso eu acho que os computadores ainda não fazem. **PCM**

Leandro Calçada
leandro.calcada@europanet.com.br

A Melhor Hospedagem.
E O Melhor Em Banda Larga.
Só na **InternetBrasil** você encontra os melhores serviços e ferramentas para a Internet, com a melhor relação custo X benefício do mercado.
No Grupo **InternetBrasil** sua empresa tem o melhor **suporte técnico** de 3 empresas especializadas em Internet, **24 horas por dia, 7 dias por semana**!
E mais: você ainda pode contar com o apoio tecnológico de parceiros como **AT&T**, **Cisco**, **Embratel**, **Intel**, **Microsoft**, **Telefónica**, entre outros, para aproveitar tudo o que a Internet tem de melhor, e fazer ótimos negócios com milhões de consumidores - no Brasil e em todo o mundo!
InternetBrasil. Muito mais Internet. Muito mais Brasil.

Ligue: (11) **3064-1000**, **3064-5000**, **5081-9000**, ou acesse: **www.internetbrasil.com.br** e tenha as melhores soluções para seus negócios na Internet.

InternetBrasil

A Internet do seu jeito.

Empresas do Grupo Internet Brasil:

Rua Correa Dias, 184 - 11º andar
Paraíso - São Paulo - SP

Empresas Parceiras:

A gente trabalhou
tanto para construir
a melhor empresa
de hospedagem
de sites que acabou
construindo a
melhor empresa de
infra-estrutura do País.

A LocaWeb acaba de ganhar o prêmio Info 200 como a melhor empresa de infra-estrutura do Brasil.
Para comemorar, vamos fazer o que a gente mais gosta: continuar
trabalhando para construir uma empresa cada vez melhor para nossos clientes.

www.locaweb.com.br - São Paulo: (11) 3049.1166 - Demais regiões: 0800 555.932

EugenioWG